



# ANYSEC-日志审计系统使用说明书



版权所有:深圳市中科网威科技有限公司





#### 声明

本公司对本手册的内容在不通知用户的情况下有更改的权利。 其版权归深圳市中科网威科技有限公司所有。 未经本公司书面许可,本手册的任何部分不得以任何形式手段复制或传播。

#### NOTICES

Shenzhen Anysec-Tech Company Limited reserves the right to make any changes in specifications and other information contained in this publication without prior notice and without obligation to notify any person or entity of such revisions or changes.

© Copyright 2009 -2012 by Anysec-Tech. Co., Ltd. All Right Reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without express written permission of Anysec Co., Ltd.

ANYSEC 是深圳市中科网威科技有限公司注册商标。所有其他商标均属于有关公司所有



目录	
----	--

	初始化配置		
	1.1 Web 管理		
	1.2用户初始账户和密码.		
	1.3 权限划分		
<u> </u>	首页		
三.	分析		
	3.1 添加分析组		
	3.2 添加已存在的图表		
	3.3 添加自定义图表		
	3.4 自定义图表预览功能.		
	3.5 自定义图表查询统计条	条件	
	3.6 编辑自定义图表		
四.	审计		
	4.1日志查询		
	4.1.1 选择过滤关键字	۲	
	4.1.2 全文搜索		
	4.1.3 钻取关联数据.		
	4.1.4 保存查询条件.		
	4.1.5 原始日志		
	4.2 关联事件		
	4.2.1 钻取关联事件.		
	4.3 内部审计		
五.	关系		
	5.1 关系设置		
	5.1.1 添加关系设置.		
	5.1.2 生成关系图		
	5.2 关系展示		
	5.3 关系过滤		
	5.3.1 添加关系过滤.		
	5.3.2 删除关系过滤.		
六.	用户		
	6.1 用户列表		
	6.1.1 添加用户		
	6.1.2 删除用户		
	6.1.3 导入用户		
	6.1.4 导出用户		
	6.1.5 模板下载		
	6.2角色列表		
	6.2.1 添加角色		
	6.2.2 删除角色		
	6.3 登录策略		
	6.3.1 添加登陆策略.		
60			
C	总机电话 0755-83658009	倊 技术支持 0755-83658229	<b><sup>1</sup>24</b> 小时技术值班热线135-1069-3536

http://www.anysec.com

◎ 深圳市龙华区观澜街道观光路 1301-80 号电子科技大学(深圳)高等研究院 3 号楼 1401



	6.3.2 删除登陆策略.		 31
	6.4 密码策略		 32
七.	资产		 . 33
	7.1 资产列表		 33
	7.1.1 资产组管理		 . 33
	7.1.2 资产添加/编辑		 . 34
	7.1.3 批量修改资产约	∄	 35
	7.1.4 批量删除资产.		 . 36
	7.1.5 模板下载		 . 37
	7.1.6 批量导入资产.		 . 37
	7.1.7 导出所有资产.		 . 37
	7.1.8 钻取资产事件.		 . 38
	7.1.9 配置 WMI		 . 38
	7.1.10 配置 JDBC		 . 39
	7.1.11 配置 SNMP		 . 41
	7.2资产类型		 42
	7.2.1 添加资产类型.		 42
	7.2.2 删除资产类型.		 43
八.	规则		 . 45
	8.1 解析规则		 45
	8.1.1 添加解析规则.		 45
	8.1.2 删除解析规则.		 46
	8.2 告警规则		 47
	8.2.1 添加告警规则.		 . 47
	8.2.2 删除告警规则.		 . 48
	8.3 过滤规则		 49
	8.3.1 添加过滤规则.		 . 49
	8.3.2 删除过滤规则.		 51
	8.3.3 启动过滤规则.		 51
	8.4 关联规则		 52
	8.4.1 添加关联规则.		 52
	8.4.2 删除关联规则.		 53
	8.4.3 启动/暂停关联	规则	 54
	8.5 授权规则		 54
	8.5.1 添加授权规则.		 55
	8.5.2 删除授权规则.		 55
九.	报表		 . 57
	9.1 添加报表		 57
	9.2 删除报表		 58
	9.3 预览/下载/生成报表.		 58
+.	告聲		 . 60
	10.1 钻取告警关联事件		 60
	10.2 告警通知		 61
Ø	总机电话 0755-83658009	😢 技术支持 0755-83658229	

http://www.anysec.com

◎ 深圳市龙华区观澜街道观光路 1301-80 号电子科技大学(深圳)高等研究院 3 号楼 1401



+	一. 网络	. 62
	11.1 组件状态	. 62
	11.2网络设置	. 62
	11.3路由设置	. 63
	11.4通信设置	. 64
	11.4.1 添加 syslog	.65
	11.4.2 编辑 SNMP	.65
	11.4.3 编辑 Session 时间	. 65
+	二. 系统	. 66
	12.1 邮箱设置	. 66
	12.2 采集器管理	. 66
	12.2.1 添加采集器	. 67
	12.3 插件中心	. 67
	12.4 知识库	. 67
	12.4.1 添加经验	. 68
	12.4.2 预览经验	. 69
	12.5 日志摘要	. 69
	12.5.1 添加日志摘要	. 69
	12.5.2 日志摘要删除	. 70
	12.5.3 日志摘要下载	. 70
	12.6 数据库导入	. 70
	12.7 日志导入	. 71
	12.8 日志监测	. 71
	12.9 数据备份	. 72
	12.9.1 手动备份	. 72
	12.9.2 自动备份	. 73
	12.9.3 自动清理	. 73
	12.9.4 自动转存	. 74
	12.10 许可信息	. 75
	12.10.1 系统升级	. 75
	12.11Ping 工具	. 76
	12.12 关机重启	. 77



# -. 初始化配置

#### 1.1 Web 管理

在浏览器地址栏输入 ip(https://192.168.1.40)(注:为出厂默认 ip)即可进行访问。 默认管理接口是 eth0。根据用户网络环境,在部署时可对访问地址进行灵活修改。

2 请先登	用户名 经录	<i>°</i>	密码	验证码	924	登录

#### 1.2 用户初始账户和密码

系统预设账户列表如下,可根据需要选择登录:

用户类型	用户名	密码
超级管理员	admin	admin123456
操作管理员	operator	operator123456
审计管理员	saudit	saudit123456
账号管理员	userManager	user123456

# 1.3 权限划分

用户类型	用户所拥有权限
超级管理员	拥有所有权限
操作管理员	除内部审计、用户管理、授权规则的所有功能
审计管理员	只有内部审计权限
账号管理员	只有用户管理权限



二. 首页

2021-02-19 15:44:23	★ ⊕ #초					
■ 状态	9.576 事件总数	事件数	<ul> <li>事件数(每秒)</li> </ul>	1	告營类型TOP5(当天)	
<u>Ⅲ</u> 分析 >	S <sup>3</sup>			0.8		
<b>阎</b> 审计 >	楼总书资			0.6		
<b>XX</b> 关系 >	<ul> <li>事件类型TOP5(当天)</li> <li>■ 其他类型</li> <li>■ 服务管理</li> </ul>			0.4	告警缆别(当天)	
各用户 >	<ul> <li>应用事件</li> <li>认证授权</li> <li>Kútadu</li> </ul>	0 0 0	0 0 0 0	0 0 0		
■资产 >	T1+E4055			0		
◇ 规则 >	告警事件趋势(月) 4k		-● 告營数量 -● 事件数量		1	1
	3k 2k				0	0.6 0.4
	1k		10 10 10 10 10 10 10 10 10 10 10 10 10 1		0	0.2
④ 网络 >	01-19 01-20 01-21 01-22 01-23 01-24 01-25 01 日志源TOP10(当天)	-26 01-27 01-28 01-29 01-30 01-31 重要告告(当天)	02-01 02-02 02-03 02-04 02-05 02-0 紧急告響(当天)	06 02-07 02-08 02-09 02-10 02-11 ( 一般告警(当天) 告響	12-12 02-13 02-14 02-15 02-16 02-17 02-18 02-19 资产分布TOP10(当天)	
③ 系统 >	25k 2k 15k 15k 16k 102,168,1,145 102,168,1,145 102,168,1,145	3.3 5.0 1.7 8.3 0.0 0 100 0	3.3 5.0 6.7 1.7 8.3 0.6 0 10.0	1 3.3 1.7 0.4 0 0 0 0		

登入系统默认进入首页即'状态'菜单项,概括显示系统主要统计信息。

# 三. 分析

点击系统右上角'编辑组'→选择添加组并填写'组名称'→点击'创建',完成添加分析组操作。如图:

2021-02-19 15:48:05	← 今日事件分析		统计范围: 近7天	<ul> <li>刷新时间: 5分钟</li> </ul>	· + 0 0
🖳 状态	事件类型分布 ③ 副質状态 一 安全男体	② 基础 2500	审计事件发生数(资产) ①		0
<ul> <li></li></ul>	osoft-Windows-TaskScheduler/Maintenace rosoft-Windows-GroupPolicy/Ciperational 以目的 成用明件 服务管理	2000	192,160,1,148	192.164.1.143	192,168,1,145
> 等保合规	基础审计事件发生数(趋势) ③	0			
> SOX合规	3000	*			
> IS027001合规 > PCI合规	2500				
<b>阎</b> 审计 >	2000				
<b>XX</b> 关系 >	1000				
冬用户 >	500				
■ 资产 >	0 2021-02-12 09:36:00 2021-02-14 12:00:00 2021-02-16 14:24:00	2021-02-18 16:48:00			

※ 总机电话-- 0755-83658009∰ http://www.anysec.com



# 3.1 添加分析组

点击系统右上角'编辑组'→选择添加组并填写'组名称'→点击'创建',完成添加分 析组操作。如图:

◎ 状态 事件类型分布 ① ③	基础审计事件发生数(资产) ②		
<ul> <li>         ・ 広告報告報</li> <li>         ・ 公正報告報</li> <li>         ・ 公正報告報</li> <li>         ・ 公正成時分析         ・ 改正成時分析         ・ 反告成時分析         ・ 反告の時代         ・         ・         ・</li></ul>	2500 2000 1500 500 0 192,163,1,148	192.168.1.143	9
編辑组 操作选择:			

## 3.2 添加已存在的图表

进入菜单项'分析'的任意子项,点击右上角'添加图表'按钮,选择需要添加的图表 类型,点击'保存'完成添加。

2021-02-19 15:54:28	₩ (D) test	统计范围: 近7天 🗸 刷新时间: 5分钟
圖 状态		新增图
山分析	×	
> 基础审计		
> 系统审计		
> WEB审计		
> Windows审计		
> 流量审计		
> 等保合规		
> SOX合规		
> 15027001合规		
test		
启审计	3	
22 关系	>	
8 用户	>	
■ 资产	>	
◇ 規则	\$	
◎ 北本	2	

					客户第一用心服务	、火"
2021-02-19 15:56:47	K ( test					
圖 状态	创建图表					
止 分析 →基础审计	~	投索框	显示全部			
> 系统审计		TOP10资产事件数量排行	Î.	网络设备事件按照事件类型排行TOP10	*	
> WEB审计		高等级事件投事件突型排行 安全设备事件趋势	>	流重天系 安全设备高等级事件按照系统分类统计		
> Windows审计		网络设备高等级事件按照系统分类统计图		全网事件趋势		
> 統量重け		操作用户分布	<			
> SOX合规		网络设备事件趋势				
> IS027001合规		다 등 기 14	•		*	
> PCI合规				自定义	保存取消	
test 倉 审 计	>					
🗙 关系	>					
冬 用户	>					
<b>副</b> 资产	>					
◇ 规则	>					
會 报表	>					

# 3.3 添加自定义图表

进入菜单项'分析'的任意子项,点击右上角'添加图表'按钮,点击'自定义'进入 自定义图表界面,可选择诸如选择统计类型/X轴/Y轴/查询条件/图表样式/TOPN/时间范围等 数据统计信息,填写图表名,点击'保存创建'完成自定义图表的操作。

2021-02-19 16:04:04	K <sup>⊕</sup> test			
🖳 状态	创建图表			
<ul> <li>业 分析 →</li> <li>→ 基础审计</li> </ul>	搜索羅	显示全部 投索框	显示全部	<b>家安征奉任何奉任</b> 奉朝(1852 · ·
> 系统审计 > WEB审计 > WIndows审计 > 流量审计 > 等保合规 > SOX合规	安至收留事件起 全网事件起势 流量关系 安全设备高等级 网络设备高等级 操作用户分布 网络设备事件起	劳 事件按照系统分类统计 事件按照系统分类统计图 势	> <	高考35年11支第14支型1917 TOP16资产事件数量排行 网络设备事件按照事件类型排行TOP10
> IS027001合规 > PCI合规				自主义 保存 取消
test 启审计 >				点击自定义
XX 关系 >				
B 资产 →				
◇规则 >				
自报表 >				

2021-02-19 16:16:07		K <sup>⊕</sup> test				
፼ 状态		自定义图表				
山分析	~		图表类型:	审计事件图表	~	
> 基础审计			统计字段:	来源IP	v	
<ul> <li>&gt; 系统审计</li> <li>&gt; WEB审计</li> </ul>			X铀数据 :	来源IP	~	
> Windows审计			查询条件:	基础审计今日事件分析	✓ +	
<ul> <li>&gt; 流量审计</li> <li>&gt; 等保合规</li> </ul>			图表样式:	柱状图	v	
> SOX合规			显示数量:	TOP5	•	
> 13021001日》 > PCI合规			开启排序:	关闭	v	
test			图表名称:	请输入图表名称		
相审计	>		图表描述:	请输入图表描述		
24、天系	>					
8 用户	>					
■ 资产	>	高等级事件按事	件类型排行			3
◇ 规则	>					
自报表	>					

- 用心服务

# 3.4 自定义图表预览功能

完成添加自定义图表后,可点击'预览'查看自定义图表,点击'查看事件',可自定义 搜索条件,如下图:

自定义图表				
	图表类型:	审计事件图表	~	
	统计字段:	来源IP	~	
	X轴数据 :	来源IP	~	
	查询条件:	₩indows审计登录成功	~ +_	-
	图表样式:	柱状图	~	自定义搜索条件
	显示数量:	TOP5	~	
	开启排序:	关闭	~	
	图表名称:	请输入图表名称		
	图表描述:	请输入图表描述	<i>li</i>	
		保存创建 预览	取消	预览图表

	(手) test		
2021-02-19 16:14:52			
🔤 状态	目儿人国农		
╽ 分析 ∽	图表类型:	审计事件图表	~
> 基础审计	统计字段:	来源IP	~
> 系统审计 > WEB审计	X轴数据 :	来源IP	×
> Windows审计	查询条件:	基础审计今日事件分析	✓ +
> 流量审计 > 等保合规	图表样式:	基础前计会日事件分析 Windows面计登录成功 Windows面计登录表权 基础前计登录从证分析	
> SOX合规	显示数量:	Windows应急变更备份 Windows审计账户管理用户禁用	
> IS027001合规 > PCI合规	开启排序:	▼indova曲计第六管理运动变更 Windova面计设合理逻辑版像用户 Windova面计以合理逻辑版像用户 Windova面计定意表更面计编码姿更	选择查询条件
test	图表名称:	Windows前计应急交更用户销路交更 Windows审计账户管理用户信用 Windows市计事件趋势应用事件	
周申计 ?	图表描述:	登录成功事件 账户锁定事件	
XX 关系 >		windows审计对象访问(新) 防火场登录失败事件 August	
各用户 >		至內會計 臺家夫收事件 Windows衛计事件趋势系统事件	•
■资产 >	高等级事件按事件类型排行		۵ ۵
◇ 规则 >			
會报表 >			

田小服争

#### 3.5 自定义图表查询统计条件

点击'查看事件'自定义搜索条件,选择'确定'跳转,可根据事件过滤条件和关键字 等进行搜索,并将条件保存(需要添加查询条件名称)。再次进入自定义图表页面 '查询条 件'项选择刚才添加的条件,可点击'预览'查看图表,也可点击保存完成自定义图表查询 统计条件的操作。

2021-02-19 16:25	:12	₭ <sup>⊕</sup> test				
◙ 状态		自定义图表				
山分析	~	图表类型:	审计事件图表	v		
> 基础审计		统计字段:	来源IP	×		
> 系统审计		X轴数据 :	来源IP	~		
> Windows审	it	查询条件:	基础审计今日事件分析	~	+	
<ul> <li>&gt; 流量审计</li> <li>&gt; 等保合规</li> </ul>		图表样式:	柱状图	~	白定义搜索条件	
> SOX合规		显示数量:	TOP5	~		
> IS027001台 > PCI合规	,规	开启排序:	关闭	×		
test		图表名称:	请输入图表名称			
倉审计	>	图表描述:	请输入图表描述			
22 关系	>			1		
8 用户	>			保存创建 预览 取消		
<b>副</b> 资产	>	高等级事件按事件类型排行				63
♦ 规则	>					
自报表	>					



2021-02-19 16:32:3	7	K <sup>⊕</sup> test					
🖳 状态		自定义图表					
山 分析	~	图表类型	: 审计事件图表	v			
> 基础审计		统计字段	: 来源IP	~			
> 系统审计 > WEB审计		X轴数据	: 未源IP	v	·		
> Windows审计		查询条件	: 基础审计今日事件分析	v	+		
<ul> <li>&gt; 流量审计</li> <li>&gt; 等保合规</li> </ul>		图表样式	: 柱状图	~		添加查询条件	
> SOX合规	-	显示数量	: TOP5	~	•]	跳转到查询条件添加页面	
> IS027001合; > PCI合规	<sup>9</sup> C	开启排序	: 关闭	~			
test		图表名称	: 请输入图表名称				
自审计	>	图表描述	请输入图表描述		]		
22 关系	>						
各 用户	>			保存创建 预览 取消			
<b>三</b> 资产	>	高等级事件按事件类型排行					63
◇ 規 则	>						
	>						









2021-02-19 16:53:22	₭ <sup>⊕</sup> test		
☑ 状态	自定义图表		
山 分析 ~	图表类型:	审计事件图表	×
> 基础审计	统计字段:	未濂IP	×
> 系统审计 > WEB审计	X轴数据 :	未滿IP	•
> Windows审计	查询条件:	Windows审计鉴录成功	<b>*</b> +
> 流量审计 > 等保合规	图表样式:	主机设备高风险事件 防火墙围筋访问事件 账户防建事件 网络边卡事件	•
> SOX合规 > ISO27001合规	显示数量:	王机设备量录失败事件 账户翻读事件 Vindova审计服务进程服务启动	
> PCI合规	开启排序:	防火墙策略更改單件 ¥indowa审计系统管理系统事件 立团的事件	
test	图表名称:	an a	
	图表描述:	1717年後末趙渓 19215月9年 記ड四時年 記ड題後渓	2 新建的查询条件
各用户 >		州「金永大郎」 信息 安全 もpt	TT ALE HEAT
<b>副</b> 资产 >	流量关系 ④		- @
◇ 规则 >			
會报表 >			

# 3.6 编辑自定义图表

进入图表可拖动状态→点击编辑图表→点击保存完成编辑自定义图表的操作。









# 四. 审计

#### 4.1 日志查询

菜单项'审计'→'日志查询'详情。



# 4.1.1 选择过滤关键字

#### 按条件过滤事件

2021-02-19 17:00:26		(← ⊕ 日志查询	_	-			保存搜索条件		保存	读取 页面刷	时间: 5分钟
▣ 状态		2		2021 02 10 161400		2021 02 10 16 29 00	200	02 18 16 12 00		2021.02.1	0 16/56/00
山分析	>	2021-02-19 16:00:00		2021-02-19 16:14:00		2021-02-19 10:20:00	202	1-02-19 16:42:00		2021-02-1	9 16:56:00
D m v			◆ 事件列表								0
图审计	×	□ 来源IP	事件名称	事件类型	事件级别	接收时间	资产名称	资产IP	资产类型	来源IP	目的IP
日志查询		□ 资产IP	计划任务日志	系统日志	信息	2021-02-19 16:55:08	centos7	192.168.1	Linux服务…		
搜索条件			session启动	配需状态	信息	2021-02-19 16:55:08	centos7	192, 168, 1,	Linux服务…		
关联事件		□ 日的場口 □ 東仕級制	++ session启动	配置状态	选择搜索	<b>关键字</b> 16:55:08	centos7	192.168.1	Linux服务…		
内部审计		□ 操作用户	成功	彩绘日本	信白	2021-02-18 16:45:09	contec?	102 169 1	LinuxBSm		
8 关系	>	日日的IP	session启动	和要性大	(* *	2021 02 10 10 45:00		100 100 1	1 ( BR 55		
く用户	>	□ 操作举型	中 engeione动	HCTL 1V.22	10.25	2021-02-19 10:40:08	CENTOS /	192.108.1.	Linuxary		
		□ <u>※</u> · · · · · · · · · · · · · · · · · · ·	成功	配置状态	信息	2021-02-19 16:45:08	centos7	192.168.1	Linux服务…		
圖 资 产	>		计划任务日志	系统日志	信息	2021-02-19 16:35:08	centos7	192.168.1	Linux服务…		
A 40 04			session启动 中	配置状态	信息	2021-02-19 16:35:08	centos7	192.168.1	Linux服务…		
✓ 592 贝则		□ 事件子类	session启动	配置状态	信息	2021-02-19 16:35:08	centos7	192 168 1	Linux服务…		
創报表	>	□ 资产类型	BRAD Hicrosoft-								
		□ 操作内容	Windows- BranchCache	Microsoft	信息	2021-02-19 16:26:50	vindows7	192.168.1	Windows		
▶ 告警	>	🗔 事件类型	SMB								
副网络	>	🗔 操作结果	session启动 中	配置状态	信息	2021-02-19 16:25:08	centos7	192.168.1	Linux服务…		
		🗇 资产主类	计划任务日志	系统日志	信息	2021-02-19 16:25:08	centos7	192.168.1	Linux服务…		
◎ 系 统	>	🗖 应用名称	session启动 成功	配置状态	信息	2021-02-19 16:25:08	centos7	192.168.1	Linux服务…		
		<u> </u>	计划任务日志	系统日志	信息	2021-02-19 16:15:08	centos7	192, 168, 1,	Linux服务…		



2021-02-19 17:04:56		🗲 🕀 日志査询					保存打	搜索条件		保存	an 页面刷新	时间: 5分钟
		●条件选择 多选 *	事件列表									® ₽ ₽
🖳 状态		□ 来源IP	事件名称	事件类型	事件级别	接收时间	ÿ	资产名称	资产IP	资产类型	来源IP	目的IP
山分析	>	192.168.1.148(···· 25	计划任务日志	系统日志	信息	2021-02-19 17:06:09	c	entos7	192.168.1	Linux服务…		
启审计	~	192.168.1.145( 16	计划任务日志	系统日志	信息	2021-02-19 17:06:09	c	entos7	192.168.1	Linux服务…		
日志杳询		□ 来源端口	计划任务日志	系统日志	信息	2021-02-19 17:06:09	c	entos7	192.168.1	Linux服务…		
搜索条件		🗀 目的端口	计划任务日志	系统日志	信息	2021-02-19 17:06:09	c	entos7	192.168.1	Linux服务…		
关联事件		□ 事件级别	session启动 中	配置状态	信息	2021-02-19 17:06:09	c	entos7	192.168.1	Linux服务…		
内部审计		□ 操作用户	计划任务日志	系统日志	信息	2021-02-19 17:06:09	c	entos7	192.168.1	Linux服务…		
22 关系	>	<ul> <li>目的IP</li> <li>操作举型</li> </ul>	session启动 成功	配置状态	信息	2021-02-19 17:06:08	c	entos7	192.168.1	Linux服务…		
Q E D	>	□ 资产类别	计划任务日志	系统日志	信息	2021-02-19 17:05:08	c	entos7	192.168.1	Linux服务…		
0 11		□ 事件名称	session启动 中	配置状态	信息	2021-02-19 17:05:08	c	entos7	192.168.1	Linux服务…		
📑 资 产	>	🗀 事件子类	session启动 成功	配置状态	信息	2021-02-19 17:05:08	c	entos7	192.168.1	Linux服务…		
◇ 规则	>	□ 资产类型	计划任务日志	系统日志	信息	2021-02-19 16:55:08	c	entos7	192.168.1	Linux服务…		
◎ 坦 韦	>	□ 操作内容	session启动 中	配置状态	信息	2021-02-19 16:55:08	c	entos7	192.168.1	Linux服务…		
	1	□ 事件类型	session启动 成功	配置状态	信息	2021-02-19 16:55:08	c	entos7	192.168.1	Linux服务…		
♥ 告 警	>	□ 操作结果	计划任务日志	系统日志	信息	2021-02-19 16:45:08	c	entos7	192.168.1	Linux服务…		
@ 网络	>	□ 资产主类	session启动	配置状态	信息	2021-02-19 16:45:08	c	entos7	192.168.1	Linux服务…		
-		□ 应用名称										
(3) 系统	>		15条/页 🗸				1 2 3	下一页				

#### 点击已选择的条件可删除该条件的限制。

2021-02-19 17:05:47		┝ 🕀 🕀 日志查询					保存搜索条件		保存	读取 页面刷新时间	J: 5分钟
図 状态		事件搜索 近15分钟 🗸									
		请输入关键词									۹ (i)
Ⅲ 分析	>	与 事件类型:"系统日志")与	(事件名称:"计划任	务日志"	J						
启审计	~	5									共7条
日志査询		4								-	
搜索条件		3									
关联事件		2									
内部审计		1									
🐹 关系	>	2021-02-19 16:53:00		2021-02-19 16:56:30		2021-02-19 17:00:00	2021	-02-19 17:03:30		2021-02-19 17	07:00
8 用户	>		事件列表								® ⊮ ⊫
<b>三</b> 次 立		□ 来源IP	事件名称	事件类型	事件级别	接收时间	资产名称	资产IP	资产类型	来源IP	目的IP
	,		0000) (19)		信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
◇ 规则	>		0008 8		信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
創报表	>	□ 事件级别	00083 (16)	<b>8888</b>	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
● 作 弊	>	□ 操作用户	00088 88	8888	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
		🗀 目的IP	0006 08	8888	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
(1) 网络	>	and the second se									
		□ 操作类型		盛德自思	信息	2021-02-19 17:05:08	centos7	192.168.1	Linux服务…		
③ 系 统	>	□ 操作类型 □ 资产类别	808 808 808	8905	信息	2021-02-19 17:05:08 2021-02-19 16:55:08	centos7 centos7	192.168.1 192.168.1	Linux服务… Linux服务…		

# 4.1.2 全文搜索

在事件搜索输入框内输入关键字,可查询包含关键字内容的事件,搜索结果中关键字高 亮蓝色背景显示。支持多个关键字搜索,多个关键字用'|'分割。



2021-02-19 17:10:5		₩ 🕀 🕀 日志查询					保存搜索条件		保存	读取 页面刷	新时间: 5分钟
□ 状态		事件搜索 近15分钟 🗸									
		localhost									۹ (
Ⅲ 分析	>	0								ш <b>н</b> -	+++++++++++++++++++++++++++++++++++++++
启审计	~	7								見て	<b>古技</b> 系 <sup>共10条</sup>
日志査询		5					_				
搜索条件		4					_				
关联事件		2									
内部审计		1									
发 关系	>	2021-02-19 16:57:30	1	2021-02-19 17:01:00		2021-02-19 17:04:30		1-02-19 17:08:00		2021-02-	19 17:11:30
0 田 白	`	✔条件选择 ^	事件列表								6.⊮.
0 /11 /		□ 来源IP	事件名称	事件类型	事件级别	接收时间	资产名称	资产IP	资产类型	来源IP	目的IP
📰 资 产	>	□ 资产IP	计划任务日志	系统日志	信息	2021-02-19 17:06:09	centos7	192, 168, 1,	Linux服务…		
◇规则	>	□ 来源端口	48620+	z#□+	in is.				·· mo.47		
· // //4		🗀 目的端口	计划任务口志	条统口志	日思	2021-02-19 17:06:09	centos/	192.168.1	Linux mp > f ***		
报表	>	□ 事件级别	计划任务日志	系统日志	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
-1 + #		□□ 操作用户	计划任务日志	系统日志	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
「「山川	,	🗇 目的IP	session启动 中	配置状态	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
● 网络	>	□ 操作类型	计划任务日志	系统日志	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
品素体	`	🗀 资产类别	session启动	配置状态	信息	2021-02-19 17:06:08	centos7	192.168.1	Linux服务…		
125 年 911	1	🗁 事件名称	以初	Z HO T	(* *	2021 02 10 17 05 02		100.100.1			
		□ 東仕子米	11 初世分日志	赤坑口态	10.22	2021-05-14 11:02:08	centos/	192.168.1	Linux 脉穷…		

2021-02-19 17:11:37		⊕ 日志查询     ∠021-02-19 16:57:30		2021-02-19 17:01:0	00	2021-02-19 17:04:30	保存搜索条件 2021	-02-19 17:08:00	保存	读取 页面刷新 2021-02-1	时间: 5分钟 9 17:11:30
፼ 状态		✔条件选择	▲ 事件列表								n l
<u>Ⅲ</u> 分析	>	□ 来源IP	事件名称	事件类型	事件级别	接收时间	资产名称	资产IP	资产类型	来源IP	目的IP
A = 1		□ 资产IP	计划任务日志	系统日志	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
	Ň	□ 来源端口	原始日志	:	<77≫Feb 20 0	01:01:01 [localhost] anacron[4902]:	Anacron started on 2021-02	-20			
日志査询					4						
搜索条件		□ 事件级别	资产类别	;	Linux						
关联事件		□ 操作用户	应用名称	:	anacron						
内部审计		🗇 目的IP	事件名称	:	计划任务日志						
26 关系	>	□ 操作类型	事件子类	:	其他						
0		🛅 资产类别	事件级别	;	信息						
8 用户	>	□ 事件名称	资产主类	;	主机设备						
■ 资产	>	□ 事件子类	发生时间	:	2021-02-19 1	7:06:09					
		🗅 资产类型	资产类型	3	Linux服务器_	Syslog					
◇ 規 则	>	□□ 操作内容	事件类型	:	系统日志						
創 报 表	>	□ 事件类型	日志拆解	:	< 77 > Feb 20	0 01:01:01 <b>localhost</b> anacro	n [4902]: Anacron starte	ed on 2021 - 02 -	- 20		
		□ 操作结果	计划任务日志	系统日志	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
▶ 告 警	>	🛅 资产主类	计划任务日志	系统日志	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
● 网络	>	🗖 应用名称	计划任务日志	系统日志	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
的系统	>		session启动 中	配置状态	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
			计划任务日志	系统日志	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		

# 4.1.3 钻取关联数据

点击图表的数据柱可查看该数据柱所表示的条件在一定时间范围内的数据详情。





2021-02-19 17:19:23	3	₩ 🕀 🕀 日志查询					保存搜索条件		保存	读取 页面刷新时	间: 5分钟
3 状态		事件搜索 其他 🗸 2	2021-02-19 17:06:00	2021-02-	-19 17:08:00						_
4 15		请输入关键词									ঽ
<u>II</u> 27 01		与(事件级别:"信息") 😧									
直审计	~	7									共7
日志査询		5									
搜索条件		4									
关联事件		2									
内部审计		1									
关系	>	2021-02-19 17:06:00		2021-02-19 17:06:28	3	2021-02-19 17:06:56	202	1-02-19 17:07:24		2021-02-19 1	7:07:52
,用户	>	●条件选择	事件列表								Ð
		□ 来源IP	事件名称	事件类型	事件级别	接收时间	资产名称	资产IP	资产类型	来源IP	目的IP
资产	>	一 资产IP	计划任务日志	系统日志	(RC)	2021-02-19 17:06:09	centos7	192 168 1	Linux服务…		
规则	>	□ 来源端口	计划在各口主	彩绘口士	(2)(2)	2021-02-10 17:00:00		102 149 1	t :		
- +P ==		□ 目的端口	日初日万日心	水池口本	CEP689	2021-02-19 17:00:09	Centos /	192.108.1	Linux, ję 9j ···		
TR AX	/	□ 事件级别	计划任务日志	系現日志		2021-02-19 17:06:09	centos7	192.168.1	Linux服穷…		
告警	>		计划任务日志	系统日志		2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
网络	>		session/启动 中	配置状态	68	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
1.4 - 14		□ 採TF尖里 □ ※卒米到	计划任务日志	系统日志	(iii)	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
系统	>	□ 页	session启动 成功	配置状态	68	2021-02-19 17:06:08	centos7	192.168.1	Linux服务…		

## 4.1.4 保存查询条件

搜索结果所对应的条件可在页面右上角'保存'左侧的输入框内命名,点击'保存'可 将该搜索条件保存,方便快捷查询。



2021-02-19 17:25	23	← ⊕ 日志查询					testl		保存	<sup>免取</sup> 页面刷	新时间: 5分钟
፼ 状态		事件搜索 近1个小时 🗸							1		
	>	请输入关键词									۹ ()
<u></u> 23 101		与[事件级别:"信息"] 与[	事件名称:"计划任务日	志" 🕑					点击保	存	
自审计	~	5									共日常
日志査询		4									
搜索条件 关联事件		2									
人		1									
22 关系	>	0 2021-02-19 16:24:00		2021-02-19 16:38:00		2021-02-19 16:52:00	2021	-02-19 17:06:00		2021-02-1	9 17:20:00
0 = +		●条件选择	▲ 事件列表								8 F F
		🗖 来源IP	and draft.	the file also well	ste ok en est	de diad 20	****	V#	We she add not	+ -	<b>D</b> #
<b>三</b> 资产	>	🛅 资产IP	事件名称	事件失望	事计级别	按限时间	货广省标	演广IP	货产类型	米源1P	目的IP
◇规则	>	🗋 来源端口		系统日志		2021-02-19 17:25:09	centos7	192.168.1	Linux服务…		
		🗀 目的端口		系统日志	信息	2021-02-19 17:15:09	centos7	192.168.1	Linux服务…		
	>	□ 事件级别		系统日志	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
警告 🆓	>	□□ 操作用户	HOHG HO	系统日志	(iic)	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
		🗇 目的IP	8086 8	系统日志	68	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
● 网络	>	□ 操作类型		系统日志	信息	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
③系统	>	🛅 资产类别	6086	系统日志	ti (B)	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…		
		□ 事件名称	00000	系统日志	A	2021-02-19 17:05:08	centos7	192, 168, 1, …	Linux服务…		
		E #47#									

2021-02-19 17:24:11		★ 🕀 日志查询					请选择搜索条件		•	读取	页面刷新时间:	: 5分钟	~
		事件搜索 近1个小时 🗸					账户删除事件		<b>^</b>				
🔤 状态		THE R. L. M. DO. T.					Vindovs审计服务进 时止接管教育的事件	程服务启动 ►	- E				
LL A to		请捆入大键问					N/ 福東昭史() 等 Vindovs审计系统管	理系统事件				ч (	
		与 [事件级别:"信息"] 与 [事件	牛名称:"计划任务日:	± 🖸			高风险事件			进场	山志夕川均	米戶占土	
▲ 审 计	~	5					DNS请求错误			边1年13	支系示计系	心中保干条	ŧ.
		à					ICMP错误日志			厌收			
日志宜调							错误级别日志信息						
搜索条件		2					HTTP请求错误						
关联事件		2					配置错误						
内部审计		1					用户登录失败						
数 关系	>	0 2021-02-19 16:24:00	_	2021-02-19 16:38:00	(	2021-02-19 16:52:00	信息		×	2	2021-02-19 17:20	0:00	
			0				安全		×				_
8 用户	>	✓条件选择 ▲	事件列表				test					₿.F	1r.
		□ 来源IP	事件名称	事件类型	事件级别	接收时间	test1 资产名称	资产IP	◇ ▼	来源	IP	目的IP	
〓 贤 产	>	□ 资产IP	<b>B</b> Ø <b>B</b> S	系统口士	(96)	2021-02-10 17:25:00	7	102 168 1	r:				
◇ 规则	>	□ 来源端口	(BB)	和知己心	CENTRA A	2021-02-19 17:20:09	CERLOS /	192, 100, 1,	Linux (k 2)				
*. 100 A.M.		🗀 目的端口		系统日志	信息	2021-02-19 17:15:09	centos7	192.168.1	Linux服务…				
报表	>	🛅 事件级别	00063	系统日志	(ii.e)	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…				
➡ 告 娶	>	□ 操作用户	tototototototototototototototototototo	系统日志	(É®)	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…				
		🗇 目的IP	00008	系统日志	(88)	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…				
● 网络	>	🗀 操作类型	00088	系统日志	(86)	2021-02-19 17:06:09	centos7	192.168.1	Linux服务…				
(6) 系 结	>	🗀 资产类别	COD(#G)	系统日本	6969	2021-02-10 17:06:09	contec7	102 169 1	Linux				
500 AN 196		□ 事件名称		37 M L 42	111111	2021 02 19 17:00:09	Centos /	152.100.1.	LINK MC 21				
		□ 東件工業		系统日志	借慮	2021-02-19 17:05:08	centos7	192.168.1	Linux服务…				

# 4.1.5 原始日志

查看原始日志:菜单项'审计'→'日志查询'→'日志拆解'。

※ 总机电话-- 0755-83658009 http://www.anysec.com



2021-02-19 17:36:30		₩ 🕀 🕀 日志查询					保存搜索条件		保存	读取 页面刷第	时间: 5分钟	
网状太		●条件选择	▲ 事件列表								rs I	Z JA
1/1/364		□ 来源IP	事件名称	事件类型	事件级别	接收时间	资产名称	资产IP	资产类型	来源IP	目的IP	
山分析	>	□ 资产IP	计划任务日志	系统日志	信息	2021-02-19 17:35:08	centos7	192, 168, 1,	Linux服务…			
启审计	~	□ 来源端口	session启动	和單件太	(注意)	2021 02 10 17 25 00	7	100 100 1	11			
		🗀 目的端口	<u>ф</u>	配置机器	间思	2021-02-19 17:35:08	centos/	192.168.1	Linux (R 95 ····			
日志査询		□ 事件级别	session 启动 成功	配置状态	信息	2021-02-19 17:35:08	centos7	192.168.1	Linux服务…			
搜索条件		□ 操作用户	Microsoft- Windows-	Microsoft	信息	2021-02-19 17:26:51	windows7	192, 168, 1, …	Windows			
关联事件		🛅 目的IP	BranchCache SNB									
内部审计		□ 操作类型	计刻任务日志	系统日志	信息	2021-02-19 17:25:09	centos7	192.168.1	Linux服务…			
22 关系	>	🗁 资产类别	原始日志	:	<78>Feb 20 01:	:20:02 localhost CROND[5070]: (ro	ot) CMD (/usr/lib64/sa/sal	1 1)				
<b>久</b> 用户	>	🗋 事件名称	资产类别	:	Linux							
0		□ 事件子类	应用名称	:	CROND							
<b>三</b> 资产	>	□ 资产类型	事件名称	:	计划任务日志							
◇规则	>	□ 操作内容	事件子类	:	其他							
•		□ 事件类型	事件级别	:	信息							
报表	>	□ 操作结果	资产主类	:	主机设备							
▶ 告 警	>	□ 资产主类	发生时间	:	2021-02-19 17:	:25:09						
		🗖 应用名称	资产类型	:	Linux服务器_Sy	rslog						
● 网络	>		事件类型	:	系统日志							
<₿ 系 統	>		日志拆解	:	< 78 > Feb 20	01:20:02 localhost CROND [	5070]: (root) CMD (/usr	/ lib64 / sa / sa	1 1 1)			
			▼ session启动 中	配置状态	信息	2021-02-19 17:25:09	centos7	192.168.1	Linux服务…			

## 4.2 关联事件

查看关联事件:菜单项'审计'→'关联事件'。

2020-06-11 10:22:1	1	★ <sup>(1)</sup> 关联事件					
园 状态		关联事件列表 搜索关键词	Q				
- VOD		事件名称	创建时间	开始时间	结束时间	教量	操作
山分析	>	▲ 同源頻繁登录失敗	2020-03-10 15:38:32	2020-03-10 15:33:32	2020-03-10 15:38:32	13	0
启审计	~	🛕 暴力破解成功	2020-03-10 15:38:32	2020-03-10 15:33:32	2020-03-10 15:38:32	13	0
日志查询		📤 多次登录失败	2020-03-10 15:38:32	2020-03-10 15:33:32	2020-03-10 15:38:32	13	<b></b>
搜索条件	_	⚠️ 尝试登录失败	2020-03-10 15:38:32	2020-03-10 15:33:31	2020-03-10 15:38:31	13	۲
关联事件				i -			共计 4 条
内部审计							
<b>X</b> 关系	>						
<b>冬</b> 用户	>						

# 4.2.1 钻取关联事件

点击关联事件列表左侧'查看'图表,可查看该关联事件的详情。

	R Anys	ec te		a logy
客户	·第一	用心	い服	务

2020-06-11 10:23:08	3	★ <sup>美联事件</sup>							
回 状态		关联事件列表 搜索关键	ē]	٩					
		事件名称	创建时间		开始时间	结束时间	数量		操作
Ⅲ 分析	>	▲ 同源頻繁登录失败	2020-03-	10 15:38:32	2020-03-10 15:33:32	2020-03-10 15:38:32	13		
<b>阎</b> 审计	~	🕰 暴力破解成功	2020-03-	10 15:38:32	2020-03-10 15:33:32	2020-03-10 15:38:32	13		0
日志查询		🔺 多次登录失败	2020-03-	10 15:38:32	2020-03-10 15:33:32	2020-03-10 15:38:32	13		0
搜索条件		⚠️ 尝试登录失败	2020-03-	10 15:38:32	2020-03-10 15:33:31	2020-03-10 15:38:31	13		0
关联事件					1				共计 4 条
内部审计									
<b>33</b> 关系	>								
Qпè	>								
020-06-11 10:23:55	5	(← (手) 日志查询				保存搜索条件	保存	取 页面刷新时间	: 5分钟
		事件投索 其他 • 20	20-03-10 15:33:32	2020-03-10 15:38:32					
1/(123									۹ (
山分析	>	操作结果: 成功 事件子类:	用户登录 ) (事件类型:认	证授权 💿					
启审计	~	6							共13条
日志查询		5							
搜索条件		3				_			
关联事件		2							
内部审计		0							
<b>X</b> 关系	>	2020-03-10 15:33:30	2020-03	3-10 15:34:40	2020-03-10 15:35:50	2020-03-10 15:37:0	D	2020-03-10 15:3	3:10
冬 用 户	>	● 操作选择 ▲	事件列表						®, J⊽ .
1 2 2 2	>	□ 採1F油素	事件名称 事	件类型 事件级别	接收时间	资产名称 资产IP	资产类型	来源IP	目的IP
<b>94</b> 7		□ 事件子类	登录成功 认	证授权 信息	2020-03-10 15:37:34	珠海鸿瑞正… 192.168.	15.1 天融信防火墙	19.133.120	
◇ 规则	>	□ 来源IP	登录成功 认	证授权 信息	2020-03-10 15:37:26	珠海鴻瑞正… 192.168.	15.1 天融信防火墙	19.133.120	

### 4.3 内部审计

查看和检索内部审计事件:菜单项'审计'→'内部审计'。

2021-02-19 18:03:03									
同代太		内部审计列表 开始时间	🛅 — (结束时间	🔤 搜索关键词	٩				ß
1/352		操作用户	登录IP	模块名称	动作	操作时间	操作内容	操作结果	
山分析	>	adain	192.168.46.65	搜索条件	查询	2021-02-19 18:00:31	搜索条件查询	成功	
倉审计	~	admin	192.168.46.65	搜索条件	查询	2021-02-19 18:00:30	搜索条件查询	成功	
日志查询		admin	192.168.46.65	搜索条件	查询	2021-02-19 18:00:29	搜索条件查询	成功	
搜索条件		admin	192.168.46.65	搜索条件	查询	2021-02-19 18:00:23	搜索条件查询	成功	
关联事件	_	admin	192.168.46.65	搜索条件管理	添加	2021-02-19 18:00:12	搜索条件添加成功	成功	
内部审计		adain	192.168.46.65	关联分析	查询	2021-02-19 17:59:00	关联分析查询成功	成功	
22 关系	>	admin	192.168.46.65	关联分析	查询	2021-02-19 17:58:34	关联分析查询成功	成功	
8 用户	>	admin	192.168.46.65	关联分析	编辑	2021-02-19 17:58:34	关联分析编辑成功	成功	
■ 茶 产	>	adain	192.168.46.65	资产分析	查询	2021-02-19 17:58:30	asset数据查询成功	成功	
		adain	192.168.46.65	关联分析	查询	2021-02-19 17:58:28	关联分析查询成功	成功	
◇ 规则	>	admin	192.168.46.65	资产分析	查询	2021-02-19 17:58:22	asset数据查询成功	成功	
創报表	>	admin	192.168.46.65	关联分析	添加	2021-02-19 17:58:21	关联分析添加成功	成功	
♥ 告警	>	admin	192.168.46.65	资产分析	查询	2021-02-19 17:57:49	asset数据查询成功	成功	
<b>A</b>		admin	192.168.46.65	关联分析	编辑	2021-02-19 17:57:49	关联分析编辑成功	成功	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	>	admin	192.168.46.65	资产分析	查询	2021-02-19 17:57:39	asset数据查询成功	成功	
③ 系统	>			1 2	3 4 5 6 7	43 下一页		共计 640	) 条



# 五. 关系

# 5.1 关系设置

# 5.1.1 添加关系设置

2021-	-02-22 12:02:21		★ 🕀 关系规则列表					
[B9]	状态		关系规则列表	搜索关键词	Q			+ ×
	and the		□ 关系规则名	称	过滤日志数据	生成结果	当前关系图	操作
	分析	>						
俎	审计	>						
×	关系	~						
	关系设置							
	关系展示							
	关系过滤							
8	用户	>						
	资产	>						
$\diamond$	规 则	>						
Ē	报表	>						
	告 整	>						
	199 H	>						
÷	系 统	>						

2021-02-22 12:37:22		← ① 添加关系规则			
፼ 状态		关系模型预览 :			
山分析	>				
启审计	>				
🗙 关系	~				
关系设置					
关系展示				提交 取消	
关系过滤		关系因素			
<b>8</b> 用户	>	○ 关系名称	源节点	目的节点	操作
<b>三</b> 资产	>				
◇ 规则	>	添加关系			
會 报表	>	* 源节点 :	◎ 输入关键字查询或点击选择	<ul> <li>(点击图标设置)</li> </ul>	
警告 🍞	>	* 关系名称 :	请输入中英文、数字 最大20字符		
● 网络	>	* 目的节点 :	2. 输入关键字查询或点击选择	<ul> <li>(点击图标设置)</li> </ul>	
③ 系统	>			<b>祿</b> 定 取消	



# 5.1.2 生成关系图

021-02-22 12:39:	+1	← ⊕ 关系规则列表				
司 北本		关系规则列表 搜索关键词	Q			
		□ 关系规则名称	过滤日志数据	生成结果	当前关系图	操作
Ⅱ 分析	>	🗌 test	系统事件		1777	20
自审计	>			1		
🕱 关系	Ŷ					
关系设置						
关系展示						
天系过速						
5 用尸	>					
圖 资 产	>					
> 规 则	>					
日报表	>					
1 告 馨	>					
野 199 路	>					
♪ 系 统	>					

# 5.2 关系展示

2021-02-22 12:40:	01	▶ ① <sup>余</sup> 系展示	当前关系规则:	无数据	• 可用过滤器:	无数
◙ 状态		查询鼓器列表				
山 分析	>	<b>智无数据</b>				
启审计	>					
发 关系	~					
关系设置						
关系展示 关系过滤						
各 用 户	>					
📑 资产	>					
◇ 规则	>					
自报表	>					
警告 脅	>					
● 网络	>					
③系统	>					



# 5.3 关系过滤

# 5.3.1 添加关系过滤

2021-02-22 12:41:41		€ 关系过滤列表			
园华东		关系过滤列表 搜索关键词	٩		🚁+ ×
1023 AC323		□ 关系过滤名称	所属关系规则	描述	操作
山 分析	>	_ test	所有		1
启审计	>		1		共计 1 条
25 关系	~				
关系设置					
关系展示					
关系过滤					
8 用户	>				
■ 资产	>				
◇ 规则	>				
	~				
目报表					
● 告警	>				
() 网络	>				
③系统	>				

#### 🖌 🕀 添加关系过滤规则

* 关系过滤名称 :	请输入中英文、数字、或英文,:07	符号 最大50字符	
* 所属关系规则 :	所有		~
关系过滤描述 :	最多输入300个字符		1
* 过滤器 :	关系次数过滤器		~
* 请选择次数匹配项 :	关系产生次数大于	✔ 筛选次数	
		(∓+n	<b>近</b> 回



# 5.3.2 删除关系过滤

2021-02-22 12:42:02		₩ (1) 关系过滤列表			× 1
同 北本		关系过滤列表 搜索关键词	Q		+ <b>*</b> x
		□ 关系过滤名称	所属关系规则	描述	操作
山 分析	>	🗌 test	所有		0 🗊
眉审计	>	7	1		共计 1 条
🗙 关系	~				
关系设置					
关系展示					
关系过滤					
8 用户	>				
■ 资产	>				
◇ 報 副	>				
• m					
1 报表	>				
警告 🖓	>				
@ 网络	>				
(6) 系 结	>				
3607 CF 226					



# 六. 用户

#### 6.1 用户列表

# 6.1.1 添加用户

点击右上角'添加图标',进入添加资产界面 将添加用户各项信息填完点击提交即可。

2021	-02-22 11:10:12		▶ ⊕ 用户列表						模板下载	「导入用户」 「导出用」
	44-		用广组	用户列表	搜索关键词	Q				≝ <b>+</b> ×
	1/(25		未分组 4		用户名	用户类型	用户描述	用户分组		操作
11	分 析	>		L.	iserManager	账号管理员	只有用户管理权限	未分组		Ø
启	审计	>		s	saudit	审计管理员	只有内部审计权限	未分组		0
101	关系	>		0	operator	操作管理员	除内部审计、用户管理、授权规则的所有…	未分组		Ø
				3	admin	超级管理员	拥有所有权限	未分组		Ø
8	用户	v					1			共计 4 条
	用户列表									
	角色列表									
	登录策略									
	密码策略									
	资产	>								
$\diamond$	规则	>								
Ê	报表	>								
	告警	>								
	网络	>								
63	系 统	>								

20	21-02-22 11:10:44		₭ ⊕ 用户3	列表 / 添加用户		
	1 状态		添加用户			
L.	A 15	`	1	* 用户名	÷	请输入中英文、数字、或英文:0符号 最大20字符
	20 101			* 翌码	:	至少3个字符
Æ	目审计	>		* 确认密码	:	请重复以上密码
2	【 关 系	>		* 角色	;	■ 计管理员 ◇
٤	3 用户	~				
	用户列表		必填项	登示策略	:	第四法論会変無略 支持多式
	角色列表			邮箱	:	请输入邮符号
	室水東略 密码策略			手机号	:	请输入手扒号
8	1 资产	>		用户组归属	:	请选择用户组 不选择则不分组
~	〃 规 则	>		用户描述	:	最多输入300个字符
ſ	报表	>				h.
-	1					規文 取消
T	1 1 2	<i>.</i>				
	9 网络	>				
63	} 系 统	>				



# 6.1.2 删除用户

点击用户列表左边方框可进行多选用户,然后点击右上角'删除'图表进行多项删除。 点击用户列表右边的'删除'图标(垃圾桶),可以进行单项删除。

2021-02-22 11:1	2:29	( ⊕ 用户列表					【模板下载】 导入用户 【导出用】
		用户组 用)	户列表 搜索关键词	Q			<u> + </u> ×
Lang 11/20		未分组 5	用户名	用户类型	用户描述	用户分组	可多项删除 操作
山分析	>		userManager	账号管理员	只有用户管理权限	未分组	0
启审计	>		saudit	审计管理员	只有内部审计权限	未分组	0
₩ 关系	>		operator	操作管理员	除内部审计、用户管理、授权规则的所有…	未分组	Ø
0			admin	超级管理员	拥有所有权限	未分组	Ø
各用户	Ý		test	审计管理员		未分组	
用户列表		1			1		甲坝删除 共计 5 条
登录策略		多选工	页				
密码策略							
■ 资产	>						
◇ 规则	>						
會 报表	>						
警告 🍞	>						
● 网络	>						
③ 系 统	>						

## 6.1.3 导入用户

点击右上角'导入用户'模块,可进行用户导入。(注:导入文件必须是 xlsx 文件)

		用户组	用户列表	搜索关键词	Q			±+
1 状态		未分组 5	□ 用	户名	用户类型	用户描述	用户分组	操作
▋ 分析	>		us	erNanager	账号管理员	只有用户管理权限	未分组	Ø
事计	>		sa	audi t	审计管理员	只有内部审计权限	未分组	Ø
【 关 系	>		op	erator	操作管理员	除内部审计、用户管理、授权规则的所有…	• 未分组	Ø
			ac	hin	超级管理员	拥有所有权限	未分组	Ø
5 用户	Ÿ		🗹 te	st	审计管理员		未分组	01
用尸列表 角色列表 登录策略 密码策略						1		共计 5
资产	>							
〃 规 则	>							
报表	>							
告警	>							
) 网络	>							
》系统	>							
用户文件								
∗ 用户文	:件	: 选择文件 未选择任何	文件					

 · 技术支持-- 0755-83658229
 · 24 小时技术值班热线-----135-1069-3536
 · 25-83658229
 · 24 小时技术值班热线-----135-1069-3536
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-83658229
 · 25-836582
 · 25-836582
 · 25-83658
 · 25-83658
 · 25-83658
 · 25-836582
 · 25-836582
 · 25-83658
 · 25-83658
 · 25-83658
 · 25-83658
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-8365
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836
 · 25-836



# 6.1.4 导出用户

点击右上角'导出用户'功能,可以进行导出用户,对系统用户进行备份。

202:	1-02-22 11:17:11		← ⊕ 用户列表						模板下载	导入用户。导出用户
ल्लि	伊太		用户组	用户列	表 搜索关键词	Q				
-	(ASE)		未分组 5		用户名	用户类型	用户描述	用户分组		操作
11	分析	>			userNanager	账号管理员	只有用户管理权限	未分组		Ø
俎	审计	>			saudit	审计管理员	只有内部审计权限	未分组		Ø
×	关系	>			operator	操作管理员	除内部审计、用户管理、授权规则的所有…	未分组		Ø
0	-				admin	超级管理员	拥有所有权限	未分组		Ø
0	н Г mitaut	Ť			test	审计管理员		未分组		0 🗇
_	用户列表						1			共计 5 条
	治己为收登录策略									
	密码策略									
	资产	>								
$\diamond$	规 则	>								
	报表	>								
	告 警	>								
۲	网络	>								
63	系 统	>								

# 6.1.5 模板下载

点击右上角'模板下载'功能,直接下载'用户模板 xlsx'文件。

2021-02-22 11:17:39		▶ 🕀 🛞 用户列表				模板下载	
		用户组	用户列表 搜索关键词	Q			± +
		未分组 5	□ 用户名	用户类型	用户描述	用户分组	操作
山 分析	>		userManager	账号管理员	只有用户管理权限	未分组	Ø
自审计	>		saudit	审计管理员	只有內部审计权限	未分组	Ø
🗙 关系	>		operator	操作管理员	除内部审计、用户管理、授权规则的所有…	未分组	Ø
0 = +			admin	超级管理员	拥有所有权限	未分组	Ø
8 用户	~		test t	审计管理员		未分组	0
用户列表					1		共计 5
用巴列农							
密码策略							
畫 资产	>						
◇ 规则	>						
創 报 表	>						
12 告警	>						
● 网络	>						
③系统	>						

### 6.2 角色列表

菜单项'用户'→'角色列表'子项。进入角色列表展示页面。

😵 总机电话 0755-83658009	😢 技术支持 0755-83658229	😵 24 小时技术值班热线135-1069-3536
http://www.anysec.com	◎深圳市龙华区观澜街道观光路13	801-80号电子科技大学(深圳)高等研究院3号楼1401

Anysec technology
客户第一 用心服务

2021-02-	20 12:42:41		K⊕∄	色列表			
Fill 44-7	t-		角色列	表 搜索关键词	Q		+ ×
1/12	13			角色名称	角色描述	角色权限	操作
山分	析	>		审计管理员	只有内部审计查看权限	审计(内部审计)	
户 用 审	भ	>		账号管理员	只有用户管理功能	用户列表,用户	
数 关	系	>		超级管理员	拥有所有权限	用户列表,状态,资产,分析,告警,报表,关系,规则,系统,网络,审计,用户	
0	*			操作管理员	除内部审计、用户管理、授权规则的所…	状态, 资产, 分析, 规则(解析规则, 过滤规则, 关联规则, 告警规则), 系统, 网络, 告警, 报表, 审计(日志查询, 关联事件, 搜索条件), …	
さ用	<u></u>	~				1	共计 4 条
用	户列表						
日	运列衣 录策略						
密	码策略						
<b>三</b> 资	7 <sup>the</sup>	>					
A ±a	<b>F</b> ul	>					
¥ 55	563						
會 报	表	>					
☆ 告	警	>					
	络	>					
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	7 ale						
(9)系	彰允	>					

## 6.2.1 添加角色

点击角色列表右上角'添加'图标,进入添加角色界面,按要求填写和选择相应的添加 项→点击'提交'完成添加角色的操作。

2021-0	2-20 12:49:40		₩ 🕀 🕀 角色列表				
[57] 카	₽本		角色列表 搜索	关键词	Q		🔶 + X
	Alles .		□ 角色名称		角色描述	角色权限	操作
加分	分析	>	审计管理员	5	只有内部审计查看权限	审计(内部审计)	
倉庫	11 计	>	账号管理员	1	只有用户管理功能	用户列表,用户	
<b>X</b> *	关系	>	超级管理员	1	拥有所有权限	用户列表, 状态, 资产, 分析, 告警, 报表, 关系, 规则, 系统, 网络, 审计, 用户	
0 =	田山	~	操作管理员	1	除内部审计、用户管理、授权规则的所…	状态, 资产, 分析, 规则(解析规则, 过滤规则, 关联规则, 告警规则), 系统, 网络, 告警, 报表, 审计(日志查询, 关联事件, 搜索条件), …	
0 /	田古利志					1	共计 4 条
	角色列表						
3	登录策略						
4	密码策略						
i ĝ	资产	>					
∲ ∌	兜 则	>					
倉 #	8 表	>					
E 19	n -n						
▲ 4	<u></u> 5 擎	>					
M (1)	网络	>					
(i) #	系统	>					

## 6.2.2 删除角色

点击角色列表标题行左侧的复选框,可选中该页所有角色,点击每条角色信息左侧的复



选框则可选中该条角色信息→点击角色列表右上角'删除'按钮,系统提示:确定删除所选 项吗?点击'确定',完成批量删除角色的操作。点击每条角色信息'操作'列'删除'图标, 系统提示:确定删除此项吗?点击'确定',完成删除角色的操作。系统内置的角色不支持删 除。

約25月1         225人並出         2           約25月1         225人並出         2           約25月1         225人並出         2           約25月1         225人並出         2           約25月1         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2 <th2< th="">         2         <th2< th=""> <th2< th=""></th2<></th2<></th2<>	₩ 第 67	刘表				
9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649       9649	角色列表	搜索关	长键词	Q		+
	_ 角1	色名称		角色描述	角色权限	操作
解音電型         只有用户管理功能         用户外表、和志、京户、分析、自整、供表、关系、规则、系线、网络、自计、用户           最低電型         除片物電油、用户管理、提供规则的所         状志、京户、分析、规则《磁环规则、差载规则、系线、网络、自当、规集、本体、风的、系线、网络、自当、规集、由计(归主查询、关联系中,计表等件),           Local         Keine         Local         Att s           Local         Test         Keine         Keine         Att s           Local         Colal         Keine         Keine         Keine         Keine           Local         Keine         K	审i	计管理员		只有内部审计查看权限	审计(内部审计)	
超度電型         拥有有权用         用户外表、状态、逆产,分析, 者里, 报表、规则, 各技, 网站, 自当, 报表、电计, 用户           操作電型         除約部审计, 用户管理, 报表规则的所 <sup>11</sup> 状态、逆产, 分析, 我则, 低有规则, 含载规则, 各载, 网站, 各载, 规则, 系执, 网站, 白雪, 建表, 年计, 用户         1         大井 5           1         1         工         大井 5           1         1         大井 5           1         大田         大田         大田           1         1         大田         大田           1         大田         大田         大田         大田           1         大田         大田         大田         大田         大田           1         大田         大田         大田         大田         大田         大田           1         大田	贝长号	号管理员		只有用户管理功能	用户列表,用户	
指官電局         附约期前计、用户弯度、接权规则的所一         北志,京产,外析,规则(解析规则,过温规则,关联规则,高量,规则,系线,同社,含量,规表,南计(日主宣调,关联事件,进票导称),)           text         文志,用户列线,资产,分析,发列,规则,系线,网站,含量,规条,南计(日主宣调,关联事件,进票导称),)           text         文志,用户列线,资产,分析,发列,规则,系线,网站,含量,规条,南计(日主宣调,关联事件,进票导称),)           text         文志,用户列线,资产,分析,发列,规则,系线,网站,含量,规条,南计(日主宣调,关联事件,进票导称),)           text         文志,用户列线,资产,分析,关系,规则,系线,网站,含量,规条,南计,用户           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           2         2           3         3           3         3           4         5           5         5           5         5           5         5           5         5           5         5	超线	级管理员		拥有所有权限	用户列表, 状态, 资产, 分析, 告警, 报表, 关系, 规则, 系统, 网络, 审计, 用户	
No. 000-000-001 Labola         No. 000-000-001         No. 000-000-000-000         No. 000-000-000-000-000-000         No. 000-000-000-000-000-000-000-000-000-00	操	作管理员		除内部审计、用户管理、授权规则的所…	状态, 资产, 分析, 规则(解析规则, 过滤规则, 关联规则, 告警规则) , 系统, 网络, 告警, 报表, 审计(日志查询, 关联事件, 搜索条件) , …	
1     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     2     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3     3 </td <td>tes</td> <td>st</td> <td></td> <td></td> <td>状态, 用户列表, 资产, 分析, 关系, 规则, 系统, 网络, 告警, 报表, 审计, 用户</td> <td>0</td>	tes	st			状态, 用户列表, 资产, 分析, 关系, 规则, 系统, 网络, 告警, 报表, 审计, 用户	0
Non-on-on-on-12:00:00					1	共计 5 务
W21-02-20 12:00:00       ● 角色技術 / 移动角色         ● 小花       ● 小花       ● 小角色合称       : text         ● 東井       >       ● 白田村       ● 白田村       ● 白田村         ● 小月       ● 二       ● 白田村       ● 白田村       ● 白田村         ● 小月       ● 二       ● 白田村       ● 白田村       ● 白田村       ● 白田村         ● 小田村       ● 山村       ● 二       ● 二       ● 二       ● 二         ● 小田村       ● 山村       ● 二       ● 二       ● 二       ● 二         ● 小田村       ● 二       ● 二       ● 二       ● 二       ● 二         ● 小田村       ● 二       ● 二       ● 二       ● 二       ● 二         ● 小田村       ● 二       ● 二       ● 二       ● 二       ● 二         ● 小田村       ● 二       ● 二       ● 二       ● 二       ● 二       ● 二         ● 小田村       ● 二       ● 二       ● 二       ● 二       ● 二       ● 二       ● 二         ● 小田村       ● 二       ● 二       ● 二       ● 二       ● 二       ● 二       ● 二         ● 小田村       ● 二       ● 二       ● 二       ● 二       ● 二       ● 二       ● 二         ● 小田村       ● 二       ● 二       ● 二       ● 二 <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td></t<>						
秋花         秋花         法加倫           山 分析         次花         金部         *角色名称 : text           山 分析         四声         角色4路 : text         角色4路 : text           白 声         四 关系         角色4路 : 記参仙入300个字符           山 大系         四 共雨         月月月           山 月月         四 天系         月月月           山 月月         四 天系         田 瑞社           山 月月         四 馬森         10 原品           山 市社         田 市社         日 用月           山 泉川         山 川         山 川           山 山 川         山 川         山 川           山 山 川         山 川         山 川           山 山 山         山 川         山 山           山 山 山         山 山         山 山           山 山 山         山 山         山 山           山 山 山         山 山         山 山           山 山 山 <td< td=""><td>1-02-20 12:50:5</td><td></td><td>🖌 🕀 角色列表 / 添加角色</td><td></td><td></td><td></td></td<>	1-02-20 12:50:5		🖌 🕀 角色列表 / 添加角色			
● 小水谷       ● 金部         ● 小水谷       ● 花本         ● 小水谷       ● 花本         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二         ● 市 汁       ● 二			权限信息	添加角色		
山 分析     秋志     秋志     小丸こか     小丸こか       □ 分析     □ 分析     □ 分析     ●       図 キ 计     >     □ 分析       図 大系     >     □ 光系       □ 規則     □ 石段       ● 用クガ表     □ 石段       ● 白沙末     □ 原時       ● 白泉     □ 月       ● 白泉     □ 月       ● 白泉     □ 月	状态		全部	* 角色名称 · test		
角壁炉     角色描述     最多单从300个字符       図 关系     □ 分析     □ 光系       □ 規用     □ 規用       月 月 水     □ 路段       月 月 水     □ 路段       日 月 水     □ 路段       1 日 彩     □ 日       1 日 彩     □ 日       1 日 彩     □ 日       1 日 彩     □ 日       1 日 形     □ 日       2 見 別     □ 日       2 見 別     ○ 日	分析	>	状态			
■ # #     □ 分析       ■ 大系     □ 大系       □ 人用     □ 人用       ● 用 户 列表     □ 市時       ● 合常     ○ 古特       ● 公 規 列     □ 用       ● 成 产     ○	审计	>	面 资产	角色描述 : 最多输入:	300个字符	
X     大     □ 元与       2     用户     >       用户     >       用户列表     □ 网站       角色列表     □ 网站       角色列表     □ 网站       査告     □ 用       資子洗給     □ 前日       資子洗給     □ 用	TT VI		■ 分析		1	
□ 元川       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二       □ 二	关系	>	王天新	权限管理 : 请选访问	权限 不选择则不授权	
A / V     田 / (1)       用 / 月 / 月 / 月 / 月 / (1)     □ □ □ □ □ □       角 色 / 月 / 月 / (1)     □ □ □ □ □       登 泉 荒 昭     □ □ □ □ □       密 呉 荒 昭     □ □ □ □       (1)     □ □ □ □       (1)     □ □ □	田户	~	11 双则	-	A	
用戶列表     田戸城     日戸城       介色列表     日 音響     点击选择权限       登录策略     日 第十       審 段 斧     日 用戶			1 条统		「「「」「「」「」「」「」「」「」「」「」「」「」「」「」「」「」「」「」」「」「	
角色列级     田市町     点击选择权限       登录策略     □ 規未     二 二       密码策略     □ 二     二 二       ● 規則     >     -	用户列表	-	国 网络 吉 牛幣			
盘 张 萊 紹 · · · · · · · · · · · · · · · · · ·	角色列表				点击选择权限	
<ul> <li>         · · · · · · · · · · · · · · ·</li></ul>	登录策略		国家社			
■ 资产 > <sup>□ ////</sup> ◇ 规则 > ② 根本 >	密码策略					
↓ 规则 >	资产	>				
ана у	规则	>				
	47 ×					

#### 6.3 登录策略

#### 6.3.1 添加登陆策略

点击登录策略列表右上角'添加'图标,进入添加登录策略界面,按要求填写和选择相应的添加项→点击'提交'完成添加登录策略的操作。



		Ke a	2.00 MT					_	_			
☑ 状态		登录策略列表 搜索并	¢键词	٩								
山分析	>	□ 策略名称		策略描述	策略状态		IP区域	日期段		日期选择	时间段	操作
		test t			允许策略		192.168.1.150-192.168	无		无	无	01
<b>宮</b> 审 计	>						1					共计 1
<b>X</b> 关系	>											
8 用户	~											
用户列表												
角色列表	-											
登录策略												
四时从时												
◇ 规则	>											
創报表	>											
▶ 告警	>											
角网络	>											
业 分 析		a. Mean and all	:	tset1								
2 审计	>	策略类型	:	tset1 允许策略 						~		
29 审计 28 关系	> > >	策略共型	:	tsetl 允许策略 最多输入300个字符					ii	×		
21 审计 33 关系 8 用户 用户列表	> > >	<ul> <li>東歐古伊</li> <li>策略类型</li> <li>策略描述</li> <li>* IF地址/段</li> </ul>	:	tset1 <b>允许策略</b> 最多输入300个字符 例:192.168.1.1-192.16	18. 1. 2;192. 188. 1. 2				ĥ	~		
<ul> <li>(2) 审 计</li> <li>(3) 关系</li> <li>(4) 关系</li> <li>(5) 用 户</li> <li>(7) 用户列表</li> <li>(角色列表)</li> </ul>	>	<ul> <li>末星日存</li> <li>東範失型</li> <li>東範描述</li> <li>* IF地址/段</li> <li>* 日期段</li> </ul>	:	tset1 九许编辑 最多输入300个字符 例: 192,168.1.1-192,16 例: 2016-01-01	18. 1. 2;192. 168. 1. 2	M	例:2016-01-02		î. Î.	•		
<ul> <li>(2) 审 计</li> <li>(2) 关 系</li> <li>(3) 关 系</li> <li>(4) 用 户</li> <li>(4) 刑</li> <li>(5) 刑</li></ul>	> > ~	<ul> <li>第4日時</li> <li>第6表型</li> <li>第6表型</li> <li>第6表述</li> <li>* 1F地山/段</li> <li>* 日期段</li> <li>* 日期段</li> </ul>	:	tset1 允许编辑 最多输入300个字符 例: 192.168.1.1-192.16 例: 2016-01-01 □周-   周二	38. 1. 2;192. 168. 1. 2 □ <b>/8</b> Ξ	] ] 周四	例:2016-01-02 □周五	<ul> <li>周六</li> </ul>		~		
<ul> <li>(2) 申 计</li> <li>(3) 关 系</li> <li>(4) 关 系</li> <li>(5) 用 户 户 列 表表</li> <li>(5) 登录项策略</li> <li>(7) 密 元</li> </ul>	> > ~	<ul> <li>第4日時</li> <li>第4日時</li> <li>第4時法述</li> <li>11時地址/段</li> <li>4日期段</li> <li>4日期後</li> <li>4日期後</li> <li>4日期後</li> </ul>	:	tset1 先许編結 最多输入300个字符 例:192.168.1.1-192.16 例:2016-01-01 	18, 1, 2; 192, 198, 1, 2 JQE	ارتان سرور ارتار	例:2016-01-02 □周五 例:02:00:00	_ 周六	·/· ·/·	~		
(2) 申 计 (3) 末 系 (4) 方 系 (5) 用 户 (7) 用 户 (7) 月 (7) 10 (7) 10 (7) 10 (7) 10 (7) 10 (7) 10 (7) 10 (7) 10 <td>&gt; &gt; &gt;</td> <td><ul> <li>末曜世神</li> <li>菜畦美型</li> <li>菜畦建述</li> <li>* IF地址/段</li> <li>* 日期段</li> <li>* 日期送择</li> <li>* 町间段</li> </ul></td> <td>:</td> <td>tset1 九许操結 最多输入300个字符 例: 192.168.1.1-192.10 例: 2016-01-01 の用ー の周二 例: 01:00:00</td> <td>)8, 1, 2;192, 168, 1, 2 □ <b>/</b>和三</td> <td>99 - 13) 93</td> <td>例: 2016-01-02 □周五 例: 02:00:00</td> <td>_ <b>周</b>大</td> <td>. МЕ</td> <td>~</td> <td></td> <td></td>	> > >	<ul> <li>末曜世神</li> <li>菜畦美型</li> <li>菜畦建述</li> <li>* IF地址/段</li> <li>* 日期段</li> <li>* 日期送择</li> <li>* 町间段</li> </ul>	:	tset1 九许操結 最多输入300个字符 例: 192.168.1.1-192.10 例: 2016-01-01 の用ー の周二 例: 01:00:00	)8, 1, 2;192, 168, 1, 2 □ <b>/</b> 和三	99 - 13) 93	例: 2016-01-02 □周五 例: 02:00:00	_ <b>周</b> 大	. МЕ	~		
<ul> <li>□ 申 计</li> <li>○ 東 计</li> <li>○ 英 系</li> <li>○ 用 户 列 表表</li> <li>○ 日 利 角色列表</li> <li>○ 密研策略</li> <li>○ 変 产</li> <li>○ 規 则</li> </ul>	> > ~	<ul> <li>第4世時</li> <li>第4世時</li> <li>第4時備送</li> <li>112地址/段</li> <li>日期段</li> <li>日期及</li> <li>日期及</li> <li>117地址/段</li> </ul>		tset1 九済発路 最多输入300个字符 例: 192.168.1.1-192.16 例: 2016-01-01 の周ー の周二 例: 01:00:00	18.1.2;192.168.1.2 一 <b>周</b> 王	) [月]四 [月] [月] [月]	例: 2016-01-02 □ 周五 例: 02:00:00	<ul> <li>周六</li> <li>規文</li> </ul>	р При При При При При При При При При Пр	•		
<ul> <li>□ 申 计</li> <li>× 系</li> <li>× 系</li> <li>用户列表表</li> <li>○ 登录策策</li> <li>○ 密码策略</li> <li>○ 资 则</li> <li>○ 规 表</li> </ul>	> > ~	<ul> <li>第4世時</li> <li>第6映型</li> <li>第6時換述</li> <li>* 117地址/段</li> <li>* 日期段</li> <li>* 日期段</li> <li>* 日期段</li> <li>* 时间段</li> </ul>	:	tsetl 先済録結 最多输入300个字符 例: 192.168.1.1-192.16 例: 2016-01-01 〇周一 〇周二 例: 01:00:00	38.1.2;192.168.1.2 □ )제Ξ	) (A) (A) (A) (A) (A) (A) (A) (A) (A) (A	例: 2016-01-02 □周五 例: 02:00:00	<ul> <li>周六</li> <li>援文</li> </ul>	, Alt	~		
2 申 计 3 年 计 5 系 8 用 户 月 户 2 予 3 元 3 元 3 元 3 元 3 元 3 元 3 元 3 元	> > > > > > >	<ul> <li>第4日は</li> <li>第4時実型</li> <li>第4時講述</li> <li>* 117地址/段</li> <li>* 日期段</li> <li>* 日期及</li> <li>* 时间段</li> </ul>	:	tset1 介许编辑 最多输入300个字符 例:192.168.1.1-192.16 例:2016-01-01 〇周一	18. 1. 2; 192. 188. 1. 2	) ) ) ) ) )	例: 2016-01-02 □周五 例: 02:00:00	□ 周六 接交	// // / 周日	~		
<ul> <li>□ 申 计</li> <li>○ 申 计</li> <li>○ 月 户</li> <li>○ 月 户</li> <li>○ 月 户</li> <li>○ 月 户</li> <li>○ 別 振客</li> <li>○ 別 振客</li> <li>○ 別 振客</li> <li>○ 別 振客</li> <li>○ 印 ○</li> </ul>	> > > > > > > > >	<ul> <li>第4日は</li> <li>第4日は</li> <li>第4日は</li> <li>第4日期後</li> <li>日期後</li> <li>日期後</li> <li>日期後</li> <li>日期後</li> <li>日期後</li> </ul>	: : : : :	tsell 先许編結 最多输入300个字符 例:192.168.1.1-192.10 例:2016-01-01 例:01:00:00 例:01:00:00	18. 1. 2; 192. 108. 1. 2 □ <b>,9</b> ]Ξ	) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	例: 2016-01-02 □ 周五 例: 02:00:00	□ 周六 授文	Дана Така Така	~		

#### 6.3.2 删除登陆策略

点击登录策略列表标题行左侧的复选框,可选中该页所有登录策略,点击每条登录策略 左侧的复选框则可选中该条登录策略→点击登录策略列表右上角'删除'按钮,系统提示: 确定删除所选项吗?点击'确定',完成批量删除登录策略的操作。点击每条登录策略'操作' 列'删除'图标,系统提示:确定删除此项吗?点击'确定',完成删除登录策略的操作。

策略者称         策略描述         策略状态         IP 区域         日期段         日期选择         时间段           test         允许策略         192.108.1.150-192.108.**         无         无         无	提升					۹.	关键词	策略列表 搜索关 <b>制</b>
test 允许策略 192.168.1.150-192.168… 无 无		时间段	日期选择	日期段	IP区域	策略状态	策略描述	策略名称
	Ø	无	无	无	192.168.1.150-192.1	允许策略		test
1	共计 1				1			

#### 6.4 密码策略

根据需求将密码策略各项设置填好,然后点击启用密码策略,点击提交。

2021-02-22 11:44:45		₩ 🐨 營銷東略		
國状态		審码策略		
山分析	>	启用密码策略 :		
@ 审计	>	* 最少小写字母个数 :	请输入最少小写字母个数	
<b>然</b> 关系	>	* 最少大写字母个数 :	请输入最少大写字母个数	
<b>久</b> 田户	~	*最少特殊字符个数 :	请输入最少特殊字符个数	
用户列表		*最少数字个数 :	请输入最少数字个数	
角色列表		*最小密码长度 :	请输入最小容码长度	
金码策略		* 審码错误次数 :	请输入错误次数	
<b>副</b> 资产	>	* 锁定时长 :	请输入损定时长(分)	ታ
◇ 规则	>	* 審码变更周期 :	请输入密码变更周期(天)	Æ
創报表	>		規交	
警告 🎝	>			
● 网络	>			
③系统	>			



七. 资产

## 7.1 资产列表

查看资产列表:菜单项'资产'→'资产列表'。

2021-02-19 18:05:0	3	₭ ⊕ 资产列表							<b>模板下载</b> 【导入资产	• 【导出资产
同作太		资产组	资产列	表 搜索关键词	Q.					≝ <b>+ ×</b>
10.32r		未分組 3		资产名称	资产IP	资产类型	日志数量	资产分组	操	作
山 分析	>			🚑 windows7	192.168.1.145	¥indows客户端	3599	未分组	0	>0 💼
自审计	>			💐 windows2012	192.168.1.143	¥indows客户端	1333	未分组	0	>0 🗇
🐹 关系	>			∆ centos7	192.168.1.148	Linux服务器_Syslog	4731	未分组	0	· Ø 💼
各用户	>			解析规则已加载 2261 行		1			ŧ	\计 3 条
■ 资产	~									
资产列表										
资产类型										
资产监控										
◇ 规则	>									
报表	>									
警 台 🖓	>									
● 网络	>									
③ 系统	>									

### 7.1.1 资产组管理

#### 7.1.1.1 编辑资产组

点击左侧资产组列表的'编辑组'图标→显示资产组编辑界面,可根据需要进行添加同级,添加下级,删除,修改资产组操作,点击'提交'完成编辑资产组操作。



2021-02-19 18	:09:14	🗲 🕀 资产列表						褀	板下載 导入资产 导出资产
□ 44+		资产组	资产列	表 搜索关键词	Q				<b>≝ + X</b>
· 小心		未分组 🕂		资产名称	资产IP	资产类型	日志数量	资产分组	操作
🔟 分析	>			₽ vindows7	192.168.1.145	Windows客户端	3599	未分组	
自审计	>			灯 vindows2012	192.168.1.143	Windows客户端	1333	未分组	◎ 1⁄2 🛱
🗙 关系	>			∆ centos7	192.168.1.148	Linux服务器_Syslog	4731	未分组	◎ 🖉 🛱
8 用户	>			解析规则已加载 2201 行		1			共计 3 条
〓 资产	~								
资产列制	表								
资产类都 资产监持	型 腔								
◇ 规则	>								
會 报表	>								
♥ 告警	>								
● 网络	>								
③系统	>								

2021-	-02-19 18:10:03		₩ ④ 资产列表						【模板下载】	导入资产	[导出资产
	状态		资产组 未分组 。	资产列表 搜索关键词	۹.					al.	+ ×
ult	分析	>	test + i Rig	<ul> <li>○ 资产名称</li> <li>→ 请输入组名称</li> <li>创建</li> </ul>	资产IP	资产类型	日志数量	资产分组		操作	
周	审计	>	子级								
×	关系	>	1								
8	用户	>									
111	资产	~									
	资产列表										
	资产类型 资产监控										
$\diamond$	规则	>									
	报表	>									
	告 警	>									
	网络	>									
63	系 统	>									

#### 7.1.2 资产添加/编辑

点击资产列表上方'添加'图标,进入添加资产界面。

点击每条资产信息'操作'列中的'编辑'图标,进入编辑资产界面,可根据需要对需 要修改的项进行编辑,点击提交完成资产编辑操作。



橫板下載	导入资产	导出资产

2021-02-19 18:10:5	55	₭ 🕀 🛞 资产列表						横板	下載 月 导入资产
同供太		资产组	Ø	产列表 搜索关键词	Q.				
1/32r		未分组。		资产名称	资产IP	资产类型	日志数量	资产分组	*
山分析	>	test 0		🗌 🔊 windows7	192.168.1.145	Windows客户端	3605	未分组	0
启审计	>			🗌 灯 windows2012	192.168.1.143	Windows客户端	1333	未分组	0
🕱 关系	>			🗌 🛆 centos7	192.168.1.148	Linux服务器_Syslog	4741	未分组	0
冬 用户	>			解析规则已加载 2261	ίŦ	1			ŧ
<b>二</b> 答 产	~								
资产列表									
资产类型									
资产监控									
◇ 规则	>								
會报表	>								
☆ 告 警	>								
✔ 告警 ● 网络	>								

2021-02-19 18:11:17		₭ ⊕ 濟产列	表 / 添加资产		
፼ 状态		漆加资产			
山分析	>		• 资产名称		请输入中英文、数字、或英文:0符号 最大50字符
眉审计	>		资产IP	:	例: 192.168.168
区 关系	>		▶ 资产类别	:	論由器 イ
8 用户	>	-	资产类型	:	Juniper論由器 🗸
<b>三</b> 资产	~		资产主类		网络设备
资产列表			• 日志编码		UTF-8 ~
资产类型		1	业务类型		请选择业务类型 最多十项
☆ 规则	>	以情而	业务端口		请按Enter健输入编口
	>	无法	采集器名称	:	本机采集器 🗸
臀 告 臀	>		资产组归属	;	请选择资产组 不选择则不分组
● 网络	>				启用JIBC 启用mm 提交 取消
③ 系统	>				
1999 - 1991 - 1975 - 1975 - 1975 - 1975 - 1975 - 1975 - 1975 - 1975 - 1975 - 1975 - 1975 - 1975 - 1975 - 1975 -					

#### 7.1.3 批量修改资产组

点击资产列表标题行左侧的复选框,可选中该页所有资产,点击每条资产信息左侧的复 选框则选中该条资产→选择想要分组的资产组名→点击添加按钮,完成批量修改资产组操作。



2021	1-02-19 18:14:21		(← ④ 资产列表	/	3				模板	下載 【导入资产】 【导出资
<b>E</b> 9	状态		资产组 提交	资产列	表 搜索关键词	٩				≝ <b>+ ×</b>
	(AC)EA		未分组。	•	资产名称	资产IP	资产类型	日志数量	资产分组	操作
11	分析	>	test 🖈		Maindows7	192.168.1.145	Windows客户端	3605	未分组	• 2 1
俎	审计	>			灯 windows2012	192, 168, 1, 143	Windows客户端	1333	未分组	• 2 1
×	关系	>	2		$\Delta$ centos7	192.168.1.148	Linux服务器_Syslog	4741	未分组	◎ 🖉 📋
8	用户	>			解析规则已加载 2261 行		1			共计 3 条
00	资产	~								
	资产列表									
	资产类型 资产监控									
\$	规则	>								
(IIII)	报表	>								
	告 警	>								
	网络	>								
63	系统	>								

#### 7.1.4 批量删除资产

点击资产列表标题行左侧的复选框,可选中该页所有资产,点击每条资产信息左侧的复选框则选中该条资产→点击资产列表右上角删除按钮,系统提示:确定删除所选项吗?点击确定,完成批量删除资产的操作。

2021-02-19 18:16:26		← ④ 资产列表							模板下载 导/	\资产 <b>-</b> 导出资
▣ 状态		资产组	资产列	表 搜索关键词	٩					<u> + ×</u>
		本分组 3 test o		资产名称	资产IP	资产类型	日志數量	资产分组		操作
加分析	,			灯 windows7	192.168.1.145	Windows客户端	3605	未分组	2	000
自审计	>	1		灯 windows2012	192.168.1.143	Windows客户端	1333	未分组		• 1 1
22 关系	>			∆ centos7	192.168.1.148	Linux服务器_Syslog	4741	未分组		000
8 用户	>			解析规则已加载 2261 行		1				共计 3 条
<b>喜</b> 资产	~									
资产列表										
资产类型 资产监控										
◇ 规则	>									
报表	>									
警告	>									
● 网络	>									
③系统	>									


# 7.1.5 模板下载

点击系统右上角'模板下载'按钮,即可下载资产模板。

2021-02-19 18:20:2	27	₭ 🕀 🛞						模板下	「載」 「导人资产」 「导出资
网状太		资产组	资产列	表 搜索关键词	Q				±+×
- Wes		未分組 3		资产名称	资产IP	资产类型	日志数量	资产分组	操作
山分析	>	test 0		灯 vindovs7	192.168.1.145	Windows客户端	3605	未分组	
启审计	>			灯 vindovs2012	192.168.1.143	Windows客户端	1333	未分组	◎ \$ \$
🐹 关系	>			∆ centos7	192, 168, 1, 148	Linux服务器_Syslog	4744	未分组	
8 用户	>			解析规则已加载 2261 行		1			共计 3 条
〓 资产	~								
资产列表									
资产类型 资产监控									
◇ 规则	>								
	>								
響 告 脅	>								
● 网络	>								
③系统	>								

# 7.1.6 批量导入资产

2021-02-19 18:21:29	★ ④ 资产列表	模板下载 导入资产 导出资产
國 状态	BAğroth 2	
Lin Asterning S	*资产文件 : 选择文件 未选择任何文件	1
🛄 ७४ ६७ 🖌 🖌	3 —— 推交 取准	
<b>阎</b> 审计 >		

# 7.1.7 导出所有资产

点击系统右上角'导出资产'按钮,即可下载包含所有资产的 xlsx 文件。

2021-02-19 18:25:07		₭ 🕀 🛞 🖗							模板1	「載」 导入资产 - 导出多	<del>م</del> رية الم
<b>同</b> 44+		资产组		资产列	大 搜索关键词	Q					
L型 状态		未分组 3			资产名称	资产IP	资产类型	日志数量	资产分组	2 操作	●出送产 ■ + × 市 ・ ク 音 ・ ク 音 ・ ク 音 ・ ク 音 ・ ク 音 い チ 新
山分析	>	test 0	/		灯 windows7	192.168.1.145	Vindovs客户端	3606	未分组		
自审计	>		1		灯 windows2012	192.168.1.143	Vindows客户端	1333	未分组	◎ / 前	
🗙 关系	>				$\Delta$ centos7	192.168.1.148	Linux服务器_Syslog	4744	未分组	◎ / 前	
0 = -					解析规则已加载 2261 行		1			共计 3 条	
8 m F	1										
■ 资产	~										



## 7.1.8 钻取资产事件

点击每条资产信息'操作'列中的'查看事件'图标,可查看该资产对应的所有事件。

★ 资产列表										模板下载 导入资产 导出资产
资产组	资产列表	搜索关键词		Q						<b>≝ + X</b>
未分组 3	_ ¥	§产名称	资	₽IP	资产类	举型	日志数量		资产分组	操作
test (		🕇 windows7	19	2.168.1.145	Windo	ws客户端	3606		未分组	
		🔰 windows2012	19	2.168.1.143	Windo	ws客户端	1333		未分组	● 1 =
	0 👔	centos7	19	2.168.1.148	Linux	服务器_Syslog	4744		未分组	• 2 1
	ĥ	¥析规则已加载 226	1 行			1				共计 3 条
日志查询							保存搜索条件		保存 读取	页面刷新时间: 5分钟 🗸
事件搜索 近1个小时 🗸										
										<b>Q</b> (i)
☆严IP: 192.168.1.145 €										共 17 条
8										
6										
4										
2021-02-19 17:26:00		2021-02-19 17	7:40:00		2021-02-19 17:54:00		2021-02-19 18:08:	00		2021-02-19 18:22:00
✓ 条件选择	*	事件列表								₿ ₣ ₽
☐ 资产IP		事件名称	事件类型	事件级别	接收时间	资产名称	资产IP	资产类型	来源IP	目的IP
□ 来源IP		停止服务	服务管理	信息	2021-02-19 18	3: windows7	192.168.1.145	∀indovs		
🗀 来源端ロ		Windows Error Reporting	应用事件	信息	2021-02-19 18	3: windows7	192. 168. 1. 145	Vindovs		
🛅 目的端口		Windows Update 代理	Microsoft-Wind	- 错误	2021-02-19 18	3: windows7	192.168.1.145	Vindovs		
□ 事件级别		Vindows Error Reporting	应用事件	信息	2021-02-19 18	3:… windows7	192.168.1.145	Vindovs		
一 操作用户		Windows Error Reporting	应用事件	信息	2021-02-19 18	3:… windows7	192.168.1.145	Vindovs		
		Windows Error Reporting	应用事件	信息	2021-02-19 18	3:… windows7	192.168.1.145	Vindovs		
		启动服务 Microsoft-	服务管理	信息	2021-02-19 18	3:… windows7	192.168.1.145	Vindows		

### 7.1.9 配置 WMI

进入编辑/添加资产界面,填写'资产名称''资产 IP'项,点击'配置选项'按钮,选择'启动 WMI'项,显示 WMI 配置界面,填写配置项内容,点击'测试连接'按钮,测试通过之后显示'提交'按钮。点击'提交'完成配置 WMI 操作。(注: Windows 必须开启 WMI 功能)



2021-02-19 18:28:0	16	★ 资产列表 / 编辑资产		
፼ 状态		编辑资产		
山 分析	>	* 资产名称	: vindovs7	
自审计	>	* 资产IP	: 192.168.1.145	
₩ 关系	>	* 资产类别	: Windows	~
各 用 户	>	* 资产类型	: Windows 客户编	v
<b>醫</b> 资产	~	* 资产主类	: 主机设备	
资产列表		*日志编码	: UTF-8	×
资产类型		业务类型	: 请选择业务类型 最多十项	
◇ 规则	>	业务端口	: 请按Enter健输入端口	
會 报表	>	采集器名称	: 本机采集器	~
♥ 告警	>	资产组归属	未分組	
● 网络	>		启用JDBC 启用VMI 规文 取消	
③系统	>			

2021-02	2-19 18:29:47		K . 201 201 201 201		
回状	态		* 资产主类	;	主机设备
LL A	+6		* 日志编码	;	۳-۶ ۷
<u> </u>	61	·	业务类型		请选择业务类型 最多十项
相軍	i it	>	业务端口	;	请按Enter储输入端口
<b>X</b> 关	系	>	采集器名称		本和平集発
名 用	户	>			
<b>三</b> 资	在产	~	<u></u>	:	赤が28
ÿ	资产列表				
8	资产类型		WIRE		
3	资产监控 1. m		* 用户名		靖输入用户名
"♥ 规	七 火川	,	* 100 M		建始 ) 亚凤
會 报	表	>	* (2, 19)		48 48 / ( ( ( ( ( ) ) )
€ 1	警	>	* 间隔(分)		请输入间隔分钟(数字)
M	络	>	监控类型	:	请选择监控类型 支持多选 •
(3) 系	统	>	* 采集开始时	间 :	当前・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
			可用性测试	-	<sub>偏用JDBC</sub> #用WIII 账准 验证通过后显示提交

# 7.1.10 配置 JDBC

http://www.anysec.com

进入编辑/添加资产界面,填写'资产名称''资产 IP'项,点击'配置选项'按钮,选 择'启动 JDBC'项,显示 JDBC 配置界面,填写配置项内容,点击'可用性测试'按钮,测试 通过之后显示'提交'按钮。点击'提交'完成配置 JDBC 操作。



2021-02-20 10:11:3	a	长 🕀 资产列表 / 编辑资产			
፼ 状态		编辑资产			
山分析	>	* 资产名称	÷	windows7	
自审计	>	* 资产IP	:	192. 108. 1. 145	
🗙 关系	>	* 资产类别	:	Windows	~
各用户	>	* 资产类型	:	Windows客户端	~
■ 资产	~	* 资产主类	:	主机设备	
资产列表		* 日志编码	:	UTF-8	~
资产类型		业务类型	:	请选择业务类型 最多十项	
◎ 规则	>	业务端口		请按Enter键输入测口	
會 报表	>	采集器名称	;	本机采集器	v
● 告警	>	资产组归属	;	(未分组)	
● 网络	>			启用JDBC 启用VIII 提交 取消	
④ 系统	>				

2021-02-20 10:12:25		资产列表 / 编辑资产     资产列表 / 编辑资产     资产列表 / 编辑资产     资产     资产     资产     资产     资产     资产     资产     资产     资产     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资     资					
🖳 状态		* 资产名称	: vindows7				
山 分析	>	* 资产IP	: 192.168.1.145				
自审计	>	* 资产类别	: Vindovs			~	
22 关系	>	* 资产类型	: Vindows客户端			~	
8 用户	>	* 资产主类	: 主机设备				
■ 資 产 资产列表	~	* 日志编码	: UTR-8			~	
资产类型		业务类型	请选择业务类型 最多十项				
资产监控		业务端口	: 请按Enter键输入端口				
▼	, ,	采集器名称	: 本机采集器			v	
■ 本本	>	资产组归属	: 未分组				点击添加JDBC
<ul> <li>(m) 网络</li> </ul>	>			禁用JDBC	启用WMI 提交 取消		
③系统	>	JDBC配置列表					• • <b>+ ×</b>
		□ 数据库类型	IP地址	王键	状态	JDBC配置名称	操作



2021-02-20 10:13	3:43	← ⑦ 资产列表 / 編編资产 添加TDBC配置	
山 分析	>	* 數据库类型	: <u>bot</u>
<b>阎</b> 审计	>	* <sup>数据库要动</sup> 选择数据库类型	1990年 Db2 * Oracle SqJ Sarver
₩ 关系	>	* 端口号	: (9]: 25565
<b>冬</b> 用户	>	* 数据库名称	: 请输入数据库名式SID
■ 资产	~	* 用户名	: 请输入用户名
资产列表		* 密码	: 请输入密码
资产类型 资产监控		* 表名	: 请输入表名
◇ 规则	>	* 主键	: 请输入主键(表的列名,该列必须是递婚的且是整颜类型,比如:ID)
會 报表	>	* 间隔	: 请输入间隔时间 分 🖌
警告 🍞	>	* 记录开始读取值	: 请输入记录开始读取值
● 网络	>	* JDBC配置名称	: 请输入JDB0的置名称
② 系统	>	* 是否开启	: 关闭 🗸
		可用性测试 🔶	#用JDB0 倉用mu 联浦 验证通过后显示提交

# 7.1.11 配置 SNMP

获取 CPU/内存/网络流量信息

进入资产→资产监控界面,选择相应资产,显示 SNMP 配置界面,填写配置项内容,点击'测试连接'按钮,测试通过之后显示'提交'按钮。点击'提交'完成配置 SNMP 操作。

2021-02-20 10:22:37	₩ ① 资产监控				
圆 状态	资产类别	资产列表 搜索关键词	Q		
	Windows				
	Linux	SNMPCO	SNMPCO	SIMPCO	
<b>阎</b> 审计 >		192.168.1.148	192.108.1.143	192.108.1.145	
<b>XX</b> 关系 >		centos7	windows2012	windows7	
8月户 >			1		共计 3 条
■ 资产 、	,				
资产列表	占去重	<b>亜配置SNMP</b> 资产			
资产类型					
资产监控					
◇规则 >					
會报表 >					
( 警击)					
● 网络 >					
③ 系统 >					



2021-02-20 10:27:49	)	₩ ① 资产监控			
回 状态		资产类别	资产列表 搜索关键词	Q	
		全部			
			centos	7未配置SNMP,点击确定跳转配置页面	
				确定 取消	
254 关系	>		Centos /	VINdovs2012 VINdovs7	
<b>久</b> 田 户	>				
-					共计 3 条
■ 资产	v			<b>只</b> 工佣定	
资产列表					
页广央型 资产监控					
◇规则	>				
11 批 衣	<i>,</i>				
♥ 告警	>				
● 网络	>				

2021-02-20 10:28:49		₩ ⑦ 资产监控 / SNMP配置			
🖾 状态		SIMP监控配置			
计分析	>	SNMP版本	:	SINF92	•
A 由 1		* 端口	:	(9]: 161	
七日 甲 미 bof	ĺ.	* 团体名	:	请输入团体名	
20, 大奈	<i>.</i>	* CPU 阈值	:	请输入1~99的整数	5
8 用 尸	>	* 内存阈值	:	请输入1~99的整数	5
· 资 产 资 产 利 考	Ý	* 磁盘阈值	:	请输入1~99的整数	5
资产类型		*发送流量阈值	;	请输入整数 最大50位数字	KB
资产监控		*接收流量阈值	:	请输入整数 最大50位数字	KB
◇ 规则	>	* 适配类型	:	¥indows	~
創 报 表	>			別述法提取道	
♀ 告 警	>			199 Malaon 6078	
• 网络	>				
③ 系 统	>				

# 7.2 资产类型

菜单项'资产'→'资产类型'子项。

# 7.2.1 添加资产类型

点击资产类型列表右上角'添加'图标,进入添加资产类型界面,资产类别和资产类型 (资产类型支持多个填写)→点击'提交'完成添加资产类型的操作。



2021-02-20 10:36:51		▶ ① 资产类型		
园 状态		资产类型列表 投索关键词 Q		<del>→+</del> ×
		□ 资产类别	资产类型	操作
山 分析	>	診由器	Juniper路由器, H3C路由器	Ø
自审计	>	See VPN	绿盟VPN,深信訳SSLVPN	Ø
🐹 关系	>	t Windows	Windows客户端, Windows系列	Ø
0		☆ 交換机	华为交换机, H3C交换机, 思科交换机, 锐捷交换机, Juniper交换机, 上海贝尔交换机, 中兴交换机, H3C_8950	
8 用户	>	🍟 上网行为	深信服上网行为管理,黑盾上网行为管理,黑盾上网行为审计	0
〓 资产	~	■ 防火墙	山石防火墙,天融信防火墙,Juniper防火墙,飞塔防火墙,华为防火墙,思科防火墙,黑盾下一代防火墙,黑盾	0
资产列表		🛃 防病毒	趋势防病毒, 黑盾防毒墙	0
资产类型		♥ 入侵防御系统	山石入侵防御系统, 天融信入侵防御系统, 绿盟入侵防御系统, 黑盾入侵防御系统, H3C入侵防御系统	Ø
资产监控		L. 数据库审计	黑盾数据库审计,建恒信安数据库审计,用30数据库审计	Ø
◇ 规则	>	◆ 网網	中铁信安单导, H3C安全隔离与信息交换系统	Ø
报表	>	● 漏洞扫描	极地漏洞扫描,建恒信安漏洞扫描,迪普漏洞扫描,H3C漏洞扫描	Ø
-1 生 数			Radware员载均衡,绿盟员载均衡,H3C员载均衡	Ø
	/	3 防毒墙	飞塔防毒墙,黑盾防毒墙,天融信防毒墙	Ø
● 网络	>	∆ Linux	ESXi,Linux服务器_Syslog	Ø
② 系 统	>	12 数据库	Mysql, SQL_Server, Oracle, DE2	Ø
			1 2 下一页	共计 24 条

2021-02-20 10:39:31		← ① 资产类型 / 编稿资产类	뽀
◎ 状态		编辑资产类型	
山谷板	>	* 资产类别	: 贻由器
		* 资产主类	: 网络设备
2目 申 计	,	* 资产类型	: Juniper路曲器 [805路曲器] 请按Enteridi编入中英文、数字、或英文:0符号 注: 输完之后按回车保存
🗙 关系	>		
<u>冬</u> 用户	>		
〓 资产	~		
资产列表	_		

### 7.2.2 删除资产类型

点击资产类型列表标题行左侧的复选框,可选中该页所有资产类型,点击每条资产类型 左侧的复选框则可选中该条资产→点击资产列表右上角删除按钮,系统提示:确定要删除吗? 点击确定,完成批量删除资产类型的操作。点击每条资产类型'操作'列'删除'图标,系 统提示:确定要删除吗?点击确定,完成删除资产类型的操作。系统内置的资产类型不支持 删除。



021-02-20 10:47:1	1	(十) 资产类型		
回 状态		资产类型列表 搜索关键词 Q		
		○ 资产类别	资产类型	操
Ⅱ 分析	>	2 法量检测	绿盟流量清洗,绿盟异常流量检测,H3C异常流量清洗系统	0
自审计	>	> 安全审计	黑盾网络安全审计系统	0
<b>2</b> 关系	>	😝 other	other,H3C智能网卡,H3C工控安全	0
		JU VEB服务器	Apache, IIS, Toncat	0
3 用户	>	\$ 终端安全	360天擎终端安全管理系统, H3C服务器安全系统	0
<b>资产</b>	~	@ 运维审计	极地运维审计, 网神运维审计, 安倍华运维审计, 鸿泰高科运维审计, 东方京海运维审计, 优炫运维审计, 中新…	. 0
资产列表		控制网关	H3C应用控制网关	0
资产类型		💐 入侵检测系统	两御入侵检测系统,琴盟入侵检测系统,黑盾入侵检测系统	0
资产监控		🎥 WEB应用防火墙	绿璧Web应用防火墙,黑雁Web应用防火墙,H3CWeb应用防火墙W2000—AK系列,H3CWeb应用防火墙W2000系列…	. 0
> 規则	>	💟 😰 test	test	6
报表	>		上一页 1 2	共计 2
◇ 告 警	>	此处可多远,然后总击有上用X进行多选删除		此久
● 网络	>			为单个册
10 10 I				际



# 八.规则

# 8.1 解析规则

菜单项'规则'→'解析规则'子项。进入解析规则列表展示页面。

2021-02-20 11:11:56	6	← ⊕ 解析规则			
同作太		解析规则列表 搜索关键词 Q			+ ×
10.325		□ 解析规则名称	解析规则创建时间	资产类型	操作
山分析	>	Tomcat日志解析规则	2019-08-28 15:12:15	Toncat	Ø
自审计	>	Apache日志解析规则	2019-08-28 15:11:24	Apache	Ø
<b>XX</b> + 系	>	Mysql日志解析规则	2019-08-28 15:10:58	Mysql	Ø
		H3C路由器解析规则	2019-07-10 14:28:18	H3C路由器	Ø
8 用户	>	黑盾上网行为审计解析规则	2019-07-03 15:48:22	黑盾上网行为审计	Ø
■ 资产	>	华清信安防火墙解析规则	2019-07-03 15:29:59	华清信安防火墙	Ø
◇ 规 则	~	H3C工控安全解析规则	2019-07-03 15:19:44	HOC工控安全	Ø
解析规则		H3C安全隔离与信息交换系统解析规则	2019-07-03 15:18:35	H3C安全隔离与信息交换系统	Ø
告警规则		H3C异常流量清洗系统解析规则	2019-07-03 15:15:28	H3C异常流量清洗系统	Ø
过滤规则		H3C智能网卡解析规则	2019-07-03 15:13:21	H3C智能网卡	Ø
关联规则		H3C服务器安全系统解析规则	2019-07-03 15:12:22	H3C服务器安全系统	Ø
授权规则		天鋭緯运維审计解析规则	2019-07-03 15:00:24	天锐锋运维审计	Ø
會 报表	>	帕拉迪运维审计解析规则	2019-07-03 14:59:11	帕拉迪运维审计	Ø
♥ 告警	>	Linux服务器_Syslog解析规则	2019-07-03 14:49:54	Linux服务器_Syslog	Ø
<b>A</b>		远江盛邦Web应用防火墙解析规则	2019-07-03 14:41:29	远江盛邦Web应用防火墙	Ø
● 网络 ◎ 系统	>	解析规则共 411 条	1 2 3 4 5 6	7 下一页	共计 97 条

# 8.1.1 添加解析规则

点击解析规则列表右上角'添加解析规则'图标,进入添加解析规则界面,填写相应的 添加项,上传解析规则文件→点击'可用性测试',测试通过则显示'提交'按钮,可点击'提 交'完成添加解析规则的操作。



2021-02-20 11:12:5	8	← ⊕ 解析规则			
回 状态		解析规则列表 搜索关键词 Q			<u> </u>
		□ 解析规则名称	解析规则创建时间	资产类型	操作
且 分 析	>	Toncat日志解析规则	2019-08-28 15:12:15	Toncat	Ø
] 审 计	>	Apache日志解析规则	2019-08-28 15:11:24	Apache	Ø
关系	>	llysql 曰志解析规则	2019-08-28 15:10:58	Mysql	Ø
		H3C路由器解析规则	2019-07-10 14:28:18	H3C路由器	Ø
,用尸	,	黑盾上网行为审计解析规则	2019-07-03 15:48:22	黑盾上网行为审计	Ø
资产	>	华清信安防火墙解析规则	2019-07-03 15:29:59	华清信安防火墙	Ø
〃 规 则	~	H3C工控安全解析规则	2019-07-03 15:19:44	H3C工控安全	0
解析规则		H3C安全隔离与信息交换系统解析规则	2019-07-03 15:18:35	H3C安全隔离与信息交换系统	Ø
告警规则		H3C异常流量清洗系统解析规则	2019-07-03 15:15:28	H3C异常流量清洗系统	Ø
过滤规则		H3C智能网卡解析规则	2019-07-03 15:13:21	H3C智能网卡	Ø
关联规则		H3C服务器安全系统解析规则	2019-07-03 15:12:22	H3C服务器安全系统	Ø
授权规则		天锐锋运维审计解析规则	2019-07-03 15:00:24	天锐锋运维审计	Ø
报表	>	帕拉迪运维审计解析规则	2019-07-03 14:59:11	帕拉迪运维审计	0
告藝	>	Linux服务器_Syslog解析规则	2019-07-03 14:49:54	Linux服务器_Syslog	Ø
		远江盛邦Web应用防火墙解析规则	2019-07-03 14:41:29	远江盛邦Web应用防火墙	Ø
网络系统	>	解析规则共 411 条	1 2 3 4 5 6	7 下一页	共计 97 -
21-02-20 11:14:5	18	★ ① 添加解析規则 添加解析規则			
1 次念		* <b>解析规则名称</b> : 请输入中英文、数字、或英	文:0符号 最大50字符		
1 分析	>				
审 计	>	* 上传规则文件 : 选择文件 未选择任何文件			
		* 资产类别 : 请选择		~	
天系	>	* 资产类型 : 请选择		~	
,用户	>				
资产	>	解析规则描述 : 最多输入300个字符			
> 规则	~		لعبر	可用性测试 取消	
解析规则					
告警规则					
अन्त के नेता जा।					

### 8.1.2 删除解析规则

点击解析规则列表标题行左侧的复选框,可选中该页所有解析规则,点击每条解析规则 左侧的复选框则可选中该条解析规则→点击解析规则列表右上角'删除'按钮,系统提示: 确定删除所选项吗?点击'确定',完成批量删除解析规则的操作。点击每条解析规则'操作' 列'删除'图标,系统提示:确定删除此项吗?点击'确定',完成删除解析规则的操作。



2020-06-11 13:12:2	1	(-) 解析规则			
回 北本	1	<b>解析规则列表</b> 搜索关键词 Q			+
	1	解析规则名称	解析规则创建时间	资产类型	采作
山 分析	>	■ Kvall下一代防火壕	2020-06-10 14:03:31	Kvall下一代防火墙	0 🖻
自审计	>	□ 亚信安全DDEI邮件网关	2020-06-09 11:00:35	亚信安全DDEI邮件网关	0 💼
<b>然</b> 关系	>	□ 珠海鸿瑞正向隔离解析规则	2020-03-03 16:28:37	珠海鸿瑞正向隔窗	0 💼
0		■ H3C安全隔高与信息交换系统解析规则	2020-01-19 18:51:05	H3C安全隔离与信息交换系统	0 1
8 用户	>	h3c入侵防御系统解析规则	2020-01-16 17:55:27	H3C入侵防御系统	0 1
<b>靈</b> 资产	>	圖 臺邦IDP解析规则	2020-01-15 23:14:26	盛邦IDP	0 6
◇ 规则	~	□ 思科踏由器	2020-01-14 20:43:40	思科路由器	ØÊ
解析规则		□ 东巽▲PT	2020-01-13 15:43:11	东巽APT	0 6
告警规则		Toncat日志解析规则	2019-08-28 15:12:15	Toncat	Ø
过滤规则		Apache日志解析规则	2019-08-28 15:11:24	Apache	Ø
关联规则		Nysql日志解析规则	2019-08-28 15:10:58	Mysql	Ø
授权规则		HSC路由器解析规则	2019-07-10 14:28:18	H3C路由器	Ø
报表	>	黑盾上网行为审计解析规则	2019-07-03 15:48:22	黑盾上网行为审计	Ø
➡ 告 警	>	华清信安防火墙解析规则	2019-07-03 15:29:59	华清信安防火墙	Ø
<b>A</b> = 40		H3C工控安全解析规则	2019-07-03 15:19:44	H3C工控安全	Ø
1997 1993 1999 1999 1999 1999 1999 1999	<i>′</i>	解析规则共 421 条	1 2 3 4 5 6 7 下一页		共计 103 #
◎ 系 统	>				

# 8.2 告警规则

菜单项'规则'→'告警规则'子项。进入告警规则列表展示页面。

2021-02-20 11:25:23		← ⊕ 告警规则						
同学大		告警规则列表 搜索关键词	<u>२</u>					+ ×
1/4325		告警名称	告警类型	告警子类	告營级别	监控频率	告謦状态	操作
山 分析	>	配置错误	配置错误	配置错误	-	5 分	<ul> <li>Image: A start of the start of</li></ul>	Ø
倉审计	>	ICMP网络不可达	网络故障	网络不可达		5 分	<li></li>	Ø
🗙 关系	>	主机高风险告警	主机高等级	高等级事件		5 分	1	Ø
0		大量用户删除	用户删除	用户删除		5 分	\$	Ø
8 m F	,	登录失败	认证授权	登录失败		5 分	2	Ø
■ 资产	>	DNS请求错误	网络故障	DNS故障		5 分	\$	Ø
◇ 規 则	~	HTTP请求错误告警	请求错误	HTTP请求错误		5 分	Ø	Ø
解析规则					1			共计 7 条
告警规则								
过滤规则								
关联规则 授权规则								
报表	>							
♥ 告警	>							
● 网络	>							
③系统	>							

## 8.2.1 添加告警规则

点击告警规则列表右上角'添加'图标,进入添加告警规则界面,按要求填写相应的添 加项→点击'提交'完成添加告警规则的操作。



	2021-02-20 11	1:26:28	<b>├ <sup>① 告警</sup></b>	规则						
	园 状态		告警规则列	表 搜索关键词	<u>Q</u>					+ ×
			0 <b>#</b>	響名称	告警类型	告響子类	告警级别	监控频率	告警状态	操作
	山分析	>	ā	置错误	配置错误	配置错误		5 分	<ul> <li>Image: A start of the start of</li></ul>	Ø
	自审计	>	10	CMP网络不可达	网络故障	网络不可达		5 分	<li></li>	Ø
	数 关系	>	E	机高风险告警	主机高等级	高等级事件		5 分	2	Ø
	0		*	量用户删除	用户删除	用户删除		5 分	<ul> <li>Image: A start of the start of</li></ul>	Ø
	8 用户	>	聋	记录失败	认证授权	登录失败		5 分	1	Ø
	<b>副</b> 资产	>	DI	<b>IS请求错误</b>	网络故障	DNS故障		5 分	\$	0
	◇ 规则	~	н	TTP请求错误告警	请求错误	HTTP请求错误		5 分	\$	Ø
	解析规	则					1			共计 7 条
	告警规	则								
	过滤规	则								
	关联规	则								
	授权规	则								
	报表	>								
	☆告警	>								
	● 网络	>								
	(2)系统	>								
_										
	2021-02-20 1	1:26:59	₩ + + + + + + + + + + + + + + + + + + +	规则 / 添加规则						
	◎ 状态		添加规则							
				- 牛躯々行 -	语绘》中英文 教史 武英女					

1 44-2		涂加规则		
一分析	>	* 告譽名称	: 请输入中英文、数字、或英文:0 符号 最大50字符	
		* 告警级别	: -#	v
目申计	,	* 监控频率	: 10 秒 ~	
关系	>	开启告警	: 🗆	
用户	>	*已存搜索	: 基础审计今日事件分析	
资产	>	* <b>搜索</b> 内容	: 干掉蚕关摊车顶	
• 规则	~	(**)1 +* m)		
解析规则	_	+ 成月天里	: 140001	
告答规则		*告警类型	: 请输入中英文、数字、或英文:()符号 最大50字符	
过滤规则 关联规则		* 告譽子类	: 请输入中英文、数字、或英文_~.:0符号 最大50字符	
授权规则		*告警条件	: 5 分 V 之内计数 < V 数字	
报表	>		機交 取油	
告整	>			

#### 8.2.2 删除告警规则

点击告警规则列表标题行左侧的复选框,可选中该页所有告警规则,点击每条告警规则 左侧的复选框则可选中该条告警规则→点击告警规则列表右上角'删除'按钮,系统提示: 确定删除所选项吗?点击'确定',完成批量删除告警规则的操作。点击每条告警规则'操作' 列'删除'图标,系统提示:确定删除此项吗?点击'确定',完成删除告警规则的操作。



2	021-02-20 11:34:30		⊬⊕≉	告警规则							多选删	余
E	3 状态		告警规	则列表	搜索关键词	Q						+ ×
				告譽名称		告警类型	告譽子类	告警级别	监控频率	告警状态		操作
1	Ⅱ 分析	>		test		test	test		10 秒	8		0
Â	自审计	>	司名洪	配置错误		配置错误	配置错误		5 分	$\checkmark$	单顶删除	0
5	<b>S</b> ¥ £	>	可多处	ICMP网络习	不可达	网络故障	网络不可达	-	5 分	0		0
	ng 25 25			主机高风险	始告警	主机高等级	高等级事件		5 分	0		0
2	3 用户	>		大量用户删	NP余	用户删除	用户删除		5 分	0		0
	■ 资 产	>		登录失败		认证授权	登录失败		5 分	0		0
	∆, ±a mi	~		DNS请求错	ίξ.	网络故障	DNS故障		5 分	0		0
	421C100			HTTP请求银	错误告警	请求错误	HTTP请求错误		5 分	0		Ø
	<u></u> 軒竹规则 告祭抑则							1				井井 9 条
	过滤规则							1				XII U A
	关联规则											
	授权规则											
	1 报表	>										
1	♀ 告 警	>										
6	● 网络	>										
Ę	즭 系 统	>										

### 8.3 过滤规则

菜单项'规则'→'过滤规则'子项。进入过滤规则列表展示页面。

2021-02-20 11:37:2	13	[← ⊕ 过滤规则			
同步本		过滤规则列表 搜索关键词	٩		0 0 <b>+ X</b>
- vos		□ 过滤规则名称	过滤条件	过滤规则状态	操作
Ⅲ 分析	>	test t	资产IP:(192.168.1.145)	Q	
自审计	>		1		共计 1 条
发 关系	>				
<b>久</b> 用 户	>				
	,				
◇ 規则	~				
解析规则					
告警规则					
关联规则					
授权规则					
會 报表	>				
警告 🖓	>				
@ @ 终	>				
(2) 系统	>				

# 8.3.1 添加过滤规则

点击过滤规则列表右上角'添加过滤规则'图标,进入添加过滤规则界面,可根据'过滤条件'和'关键字'完成过滤条件的选择,填写'过滤规则名',选择'过滤规则状态'→ 点击'提交'完成添加过滤规则的操作。



2021-02-2	0 11:48:55	K	🕂 🕀 过滤规则			
፼ 状态		过滤规	!则列表	搜索关键词		
山分枝	fi >		过滤规则 test	则名称		
启审计	+ >	0				
<b>說</b> 关 测	к >					
8月1	± >					
<b>三</b> 资产	ž >					

11:48:55		K O				
		过滤规则列表 搜索关键词	2			⊙ ® + ×
		□ 过滤规则名称	过滤条件		过滤规则状态	操作
	>	test	资产IP:(192.168.1.145)		Q	
	>			1		共计 1 条
()	>					
r.	>					
	<i>,</i>					

2021-02-20 11:50:3	3	₩ 312總規則列表 7 降加	177.98:46663			
		计动作件并称	过滤事件列表 近15分钟	<b>~</b>		
፼ 状态		□ 来源IP	请输入关键词			Q.
山分析	>	<ul> <li>资产IP</li> <li>未源端口</li> </ul>	资产名称	资产IP	时间	原始日志
日审计	>		windows7	192.168.1.145	2021-02-20 11:59:30	系统启动时间为 77591 秒。
		□ 目的MAC	windows2012	192.168.1.143	2021-02-20 11:58:38	系统启动时间为 77584 秒。
22 关系	>	□ 事件级别	centos7	192.168.1.148	2021-02-20 11:55:08	<78>Feb 20 19:50:01 localhost CROND [15270]: (root)
各用户	>	□□ 操作用户	centos7	192.168.1.148	2021-02-20 11:55:08	< 30 > Feb 20 19:50:01 localhost systemd: Starting Ses
		🗇 目的IP	centos7	192.168.1.148	2021-02-20 11:55:08	< 30 > Feb 20 19:50:01 localhost systemd: Started Sess…
篇 资产	>	🖿 MAAC	centos7	192.168.1.148	2021-02-20 11:45:08	<78>Feb 20 19:40:01 localhost CROND [15181]: (root)
公规则	~	🗔 原始日志	centos7	192.168.1.148	2021-02-20 11:45:08	< 30 > Feb 20 19:40:01 localhost systemd: Starting Ses…
		🗔 系统名称	centos7	192.168.1.148	2021-02-20 11:45:08	< 30 > Feb 20 19:40:01 localhost systemd: Started Sess
解析规则		□ 操作类型				
告警规则		🗀 服务名称				共计 8 条
过滤规则		□ 资产类别				
关联规则		🗔 事件名称				
授权规则		🛅 错误码				
會 报表	>	🗀 事件子类			6件	
		🛅 Dns响应代码				
▲ 告 警	>	□ 资产类型				
@ 网络	>	🗀 域名				
		🗔 发送字节				
⑥ 系统	>	The states of				

2021-02-20 11:57:15	₩ 🕀 🕀 过滤规则列表 / 添加	口过滤规则	
፼ 状态		1 资产IP	
山 分析 >		192.188.1.14 "localbost"	
<b>阎</b> 审计 >			
<b>XX</b> 关系 >			
各用户 >	过滤条件选择	过速事件对表 近15分钟 🗸	
■资产 >	<ul> <li>资产IP</li> <li>中源IP</li> </ul>	请输入关键词	Q

	<b>三</b> 资产	>		请输入关键词			Q.
i.			□ 来源IP	the star of the	10 th an		640±
L	◇ 规则	~	□ 来源端口	黄广石桥	wr-ir	8.7 (6)	原始日志
н	解析抑励		🗀 目的端口	centos7	192.168.1.148	2021-02-20 12:06:08	< 77 > Feb 20 20 : 01 : 02 [localhost] run - parts (/ etc / cron
	告警规则		亡 目的MAC	发生时间 :	2021-02-20加入投票条件。	3 选中点击,	点击"与"加入搜索条件
	过速规则		🗀 事件级别	原始日志 :	< 77 > Feb 20 20 : 01 : 02	localhost an - parts (/ etc / cron. ho	urly)[1538 finished Oanacron
E	关联和问	-	🗀 操作用户	centos7	192.168.1.148	2021-02-20 12:06:08	< 78 > Feb 20 20 : 01 : 02 [localhost] CROND [ 15373 ]: (root)
	授权规则		🗀 目的IP	centos7	192.168.1.148	2021-02-20 12:06:08	< 77 > Feb 20 20 : 01 : 02 [localhost] run - parts (/ etc / cron
	<u>م</u> بر ج		🗂 irnac	centos7	192.168.1.148	2021-02-20 12:06:08	<pre>&lt; 30 &gt; Feb 20 20 : 01 : 02 localhost systemd : Starting Ses<sup></sup></pre>
	一批 衣	,	🛅 原始日志	centos7	192.168.1.148	2021-02-20 12:06:08	(30)Feb 20 20:01:01 localhost systemd: Started Sess.
	♥ 告 警	>	🛅 系统名称	centos7	192.168.1.148	2021-02-20 12:05:08	< 78 > Feb 20 20:00:01 [localhost] CROND [15358]: (root)
			□ 操作类型	centos7	192 168 1 148	2021-02-20 12:05:08	(20) Ech 20 20:00:01 [con]boot systemd: Starting Sec."
	● 网络	>	🗔 服务名称				(307) PD 20 20,00,01 Contractor Systemu. Starting Ses
	5m2 7 44		□ 资产类别	centos7	192.168.1.148	2021-02-20 12:05:08	<pre>&lt;30 &gt; Feb 20 20 :00 :01 localhost systemd : Started Sess ***</pre>
	1937 奈 坑	/	門 事件タわ	centos7	192.168.1.148	2021-02-20 11:55:08	< 78 > Feb 20 19:50:01 [localhost] CROND [15270]: (root)

😢 总机电话-- 0755-83658009 ttp://www.anysec.com

😢 技术支持-- 0755-83658229 1069-3536 24 小时技术值班热线-----135-1069-3536 ◎ 深圳市龙华区观澜街道观光路 1301-80 号电子科技大学(深圳)高等研究院 3 号楼 1401

副 状态     2 違違規則當該       山 分析 >>     *过滤規則名称 : test       全 审计 >>     *过滤規則状态 : 伸止	
山分析     *过滤規制结称:     test       留申计     *过滤規制体态::     停止        國家     *     ●     ●	
<ul> <li>● 市计 &gt;</li> <li>● 成本規則状态 : 伸止 </li> <li>● 成本規則状态 : 伸止 </li> <li>● 成本規則状态 : 伸止 </li> </ul>	
回州市 / · · · · · · · · · · · · · · · · · ·	
■ 资产 > 192.168.1.1 (localhost)	

#### 8.3.2 删除过滤规则

点击过滤规则列表标题行左侧的复选框,可选中该页所有过滤规则,点击每条过滤规则 左侧的复选框则可选中该条过滤规则→点击过滤规则列表右上角'删除'按钮,系统提示: 确定删除所选项吗?点击'确定',完成批量删除过滤规则的操作。点击每条过滤规则'操作' 列'删除'图标,系统提示:确定删除此项吗?点击'确定',完成删除过滤规则的操作。

2021-02-20 12:00:41		▶ ① 过滤规则			
圖 状态		过滤規则列表 投索关键词 Q			• • + ×
		□ 过滤规则名称	过滤条件	过滤规则状态	操作
山 分析	>	✓ test	资产IP:(192.168.1.145)	Q	
启审计	>	1	1		共计 条
🐹 关 系	>	(			
8 用户	>				

### 8.3.3 启动过滤规则

点击过滤规则列表标题行左侧的复选框,可选中该页所有过滤规则,点击每条过滤规则 左侧的复选框则可选中该条过滤规则→点击过滤规则列表右上角'多选停止/多选开启'按钮, 系统提示:确定停止/开启所选项吗?点击'确定',完成批量停止/开启过滤规则的操作。点 击每条过滤规则'操作'列'开启/停止'图标,系统提示:确定停止/开启此项吗?点击'确 定',完成停止/开启过滤规则的操作。

Anysec technology	
客户第一 用心服务	

2021-02-20 12:09:3	34	★ ① 过滤規则			
大++ [23]		过滤规则列表 搜索关键词	Q		🔎 🛛 + 🗙
1/365		□ 过滤规则名称	过滤条件	过滤规则状态	操作
山分析	>	✓ test	资产IP:(192.168.1.145)	8	
自审计	>	<b>N</b>	1		共计 1 条
22 关系	>				
8 用户	>				
<b>三</b> 资产	>				
◇ 规 则	~				

# 8.4 关联规则

菜单项'规则'→'关联规则'子项。进入关联规则列表展示页面。

2021-02-20 12:10:27		(			
网状本		关联规则列表 搜索关键词	Q		⊙ ⊕ + >
- 1763B		□ 关联规则名称	关联规则创建时间	关联规则描述 关联规	谢状态 操作
山 分析	>	管理员账户登录失败	2021-02-19 17:58:34	使用管理员帐号多次登录失败	00 🖉
启审计	>	暴力破解	2019-06-28 10:54:03	同源地址对目标设备进行頻繁碳解登录并能登录… 🔗	00 0
₩ 关系	>	同源頻繁登录	2019-06-28 10:51:13	同一个源地址多次登录失败 🛷	00 Ø
冬 用 户	>			i	共计 3 条
<b>喜</b> 资产	>				
✓ 規 则 解析规则 告警规则 过滤规则	×				
关联规则					
授权规则					
創 报 表	>				
▶ 古警	>				
● 网络	>				
高 系 统	>				

# 8.4.1 添加关联规则

点击关联规则列表右上角'添加关联规则'图标,进入添加关联规则界面,按要求填写 相应的添加项→点击'下一步'进入下一环节添加,或者点击'提交'完成添加关联规则操 作。

2021-02-20 12:1	1:57	₩ 全联规则				
圖 状态		天联双则列表 投索天谜词	大联規則创建时间	关联和创模外	关联规则状态	€ <b>●</b> × ×
山分析	>	管理员账户登录失败	2021-02-19 17:58:34	使用管理员帐号多次登录失败	<i>√</i>	00 0
启审计	>	暴力破解	2019-06-28 10:54:03	同源地址对目标设备进行頻繁碳解登录并能登录…	\$	00 Ø
28 关系	>	同源頻繁登录	2019-06-28 10:51:13	同一个源地址多次登录失败	<i></i>	00 🖉
<b>8</b> 用户	>			1		共计 3 条
1 资产	>					
😢 总机目	电话	0755-83658009	😢 技术支持 0755-836	58229 🛛 🍪 24 小时技术	值班热线	135-1069-3536
🌐 http:/	//www.	.anysec.com	◎ 深圳市龙华区观澜街道	i 观光路 1301-80 号电子科技	大学(深圳)高等	研究院3号楼140



2021-02-20 12:12:20	Ke	🖹 关联规则 / 添加关联规则		
回 状态	添加	D关联规则		
LL A to			0 0	
		* 关联规则名称	请输入中英文、数字、或英文:()符号 最大50字符	
創审计	>	关联资产名称	搜索框 显示全部 搜索框 显示全部	
<b>XX</b> 关系	>		centos7	
8 用户	>		windows2012 >>	
<b>副</b> 资产	>		windows7	
◇ 规则	~			
解析规则				
告警规则		사 다구 가지 가 나는 것이 같이 않는 것이 같이 않는 것이 없다. 같이 않는 것이 없는 것이 없이 않이		
过滤规则 关联规则	-	大联争计关望	博输入州央关、数子、纵央关;1/175 顺入50子们	
授权规则		关联事件子类	请输入中英文、数字,或英文,:0符号 最大50字符	
創报表	>	关联事件名称	请输入中英文、数字、或英文,:0符号 最大50字符	
♥ 告警	>	关联事件结果	请输入中英文、数字、或英文::0符号 最大50字符	
@ 网络	>	关联资产类型	请输入中英文、数字、或英文:0符号 最大50字符	
Sa m tr		自定义源地址	例: 192.168.168.168 请按Enter键输入	
302 243 224				
2021-02-20 12:12:41	K	🕑 关联规则 / 添加关联规则		
网状态		关联事件结果	请输入中英文、数字、或英文;:0符号 最大50字符	
		关联资产类型	请输入中英文、数字、或英文::0符号 最大50字符	
1111 25 MT	<i>,</i>	自定义源地址	例: 192.168.168 请按Enter谜输入	
启审计	>	自定义源端口	例: 161;25565 (多个请以英文分号分割) 请按Enter键输入	
22 关系	>	自定义目标地址	例: 192.168.168.168;192.168.1.1 (多个请以英文分号分割) 请按Enter键输入	
8 用户	>	自定义目标端口	例:101;25505(多个请以英文分号分割)请按Enter健输入	
📰 资产	>	*时间间隔	请输入5~60的整数(分仲)	 分
◇ 規 则	~	* 事件次教	请输入学联合托次教	
解析规则		+ (8)3	()(()()()()()()()()()()()()()()()()()(	
告警规则		大健间	相相(小之所)回(32)(損化)工協力(第2)	
<b>江</b> 遮规则 关联 <u>规则</u>		* 关联事件名称	请输入中英文、数字、或英文:0符号 最大50字符	
授权规则		* 关联事件级别	信息	~
會 报表	>	* 关联规则状态		v
警 금 🖓	>	关联规则描述	最多输入300个字符	
● 网络	,		<i>h</i>	
的系统			下一步 提交 取消	
2.55 尔 列				

# 8.4.2 删除关联规则

点击关联规则列表标题行左侧的复选框,可选中该页所有关联规则,点击每条关联规则 左侧的复选框则可选中该条关联规则→点击关联规则列表右上角'删除'按钮,系统提示: 确定删除所选项吗?点击'确定',完成批量删除关联规则的操作。点击每条关联规则'操作' 列'删除'图标,系统提示:确定删除此项吗?点击'确定',完成删除关联规则的操作。

						客户第一 用心服
2021-02-20 12:17:1	2	★ ○ 关联规则				
回 状态		关联规则列表 搜索关键词	Q			<u> </u>
		□ 关联规则名称	关联规则创建时间	关联规则描述	关联规则状态	操作
山 分析	>	v test	2021-02-20 12:42:18		Q	
启审计	>	管理员账户登录失败	2021-02-19 17:58:34	使用管理员帐号多次登录失败	\$	00 /
<b>XX</b> ≠ ≅	>	✓ 暴力破解	2019-06-28 10:54:03	同源地址对目标设备进行频繁碳解登录并能登录…	\$	00 🖉 🛱
846 X 25		同源頻繁登录	2019-06-28 10:51:13	同一个源地址多次登录失败	0	00 / 11
8 用户	>					## 4
				1		2711 4

A 7410

### 8.4.3 启动/暂停关联规则

点击关联规则列表标题行左侧的复选框,可选中该页所有关联规则,点击每条关联规则 左侧的复选框则可选中该条关联规则→点击关联规则列表右上角'多选停止/多选开启'按钮, 系统提示:确定停止/开启所选项吗?点击'确定',完成批量停止/开启关联规则的操作。点 击每条关联规则'操作'列'开启/停止'图标,系统提示:确定停止/开启此项吗?点击'确 定',完成停止/开启关联规则的操作。

2021-02-20 12:25:38		₩ (1) 关联规则				
园 #本		关联规则列表 搜索关键词	Q			→⊙ © + ×
		□ 关联规则名称	关联规则创建时间	关联规则描述	关联规则状态	操作
山 分析	>	✓ test	2021-02-20 12:42:18		8	
自审计	>	管理员账户登录失败	2021-02-19 17:58:34	使用管理员帐号多次登录失败	\$	00 0
22 关系	>	/ 暴力破解	2019-06-28 10:54:03	同源地址对目标设备进行頻繁破解登录并能登录…	2	00 0
0 = 5		同源頻繁登录	2019-00-28 10:51:13	同一个源地址多次登录失败	Ø	00 🖉
8 m F	,			1		共计 4 条
■ 资产	>					
◇ 規则	~					
A22.4/* 4/8 (8-1						

### 8.5 授权规则

菜单项'规则'→'授权规则'子项。进入授权规则列表展示页面。



20	21-02-20 12:28:36		★ ① 授权规则		
6	] #**		授权規则列表 捜索关键词 Q		_+ ×
5	a 17.353		□ 授权规则名称	授权规则描述	操作
8	▋ 分 析	>	test		2 🗇
Ą	事 计	>		1	共计 1 条
8	关系	>			
٤	5 用户	>			
	圖 资 产	>			
	<ul> <li>規則</li> <li>解析規則</li> <li>告警規則</li> <li>过滤規則</li> <li>关联規則</li> <li>授权規則</li> </ul>	~			
1	一报表	>			
τ	\$ 告警	>			
	● 网络	>			
Ę	③ 系 统	>			

### 8.5.1 添加授权规则

点击授权规则列表右上角'添加'图标,进入添加授权规则界面,按要求填写和选择相应的添加项→点击'提交'完成添加授权规则的操作。



## 8.5.2 删除授权规则

点击授权规则列表标题行左侧的复选框,可选中该页所有授权规则,点击每条授权规则



左侧的复选框则可选中该条授权规则→点击授权规则列表右上角'删除'按钮,系统提示:确定删除所选项吗?点击'确定',完成批量删除授权规则的操作。点击每条授权规则'操作'列'删除'图标,系统提示:确定删除此项吗?点击'确定',完成删除授权规则的操作。

2021-02-20 12:41:34	₩ 🕀	权规则						
网步本	授权规则	1列表 搜索关键词	Q					+×
		授权规则名称			授权规则描述			操作
山 分析	>	test						0 👮
启审计	,				1			共计 1 条
<b>这</b> 关系	>							
各用户	>							
<b>资</b> 产	>							
◇ 規则	÷							
₩ ① 登录策略								
登录策略列表	搜索关键词	<u>२</u>						×
□ 策略名称		策略描述	策略状态	IP区域	日期段	日期选择	时间段	操作
💙 test			允许策略	192.168.1.150-192.168…	无	无	无	
				1				共计 1 条



九. 报表

菜单项'报表'→'报表列表'子项。进入报表列表展示页面。

2021-02-20 13:08:52		₩ 🕀 🕀 报表列表					
		报表	今日事件分析 搜索关键词	Q		开始时间	- 结束时间
□ 状态		□ 基础审计	报表名称	报表类型	已生成报表		操作
山分析	>	今日事件分析	基础审计事件发生数(资产)	内置报表	未生成报表		RO
剧审计	>	登录认证分析	基础审计事件发生数(事件子类型)	内罟报表	未生成报表		RA
		双田威勝力析	基础审计事件发生数(指数)	内罟报表	未生成报表		® A
<b>XX</b> 关系	>	□ weB审计	基础审计事件发生数(资产类型)	内罟捉表	未生成报表		B A
8 用户	>	🛅 Windows审计	至福市(1事件火土数(3) 天里)	11111KA	小王/JARA		<i>ev</i>
		□ 決量审计	室哨申计争件发生数(事件关型)		木主丸(泉衣		
■ 致产	>	等保合规	叠幅审计事件发生数(事件吸列)	内面报表	木生成接表		20
◇ 规则	>	□ SOX合规			1		共计 6 条
	~	🛅 IS027001…					
in the sec		■ PCI合規					
报表列表		□ 其他					
警告 🎝	>	自定义报表					
● 网络	>						
③系统	>						

## 9.1 添加报表

点击报表列表右上角'添加'图标,进入添加报表界面,按要求填写,上传文件,选择 需要的报表类型→点击'提交'完成添加报表的操作。

21-02-20 13:14:40						
司状态	16	表	自定义报表 搜索关键词	Q	开始时间	- 结束时间
		] 基础审计	□ 报表名称	报表类型	已生成报表	操作
分析	>	今日事件分析				
( ± 11		登录认证分析				
<b>Р</b> И		攻击威胁分析				
关系	· ·	] 系统审计				
		) WEBHHVT				
,用尸	· -	] Windows申计				
1 资产	· ·	] 流重审计				
		] 等保合规				
〃 规 则	>	]SOX合规				
1 报表	~ -	] IS027001…				
		] PCI合规				
撤农列农		〕其他				
3 告 警	> 自	定义报表 🤸				
A 107 42	<u>,</u>					
y 113 94						
多系统	>					

次応       次       回素名称       注 注注       日本       日本	1-02-20 13:15:	21	(十)报表列表 / 添加报表 添加报表			
資产     P     P%设备备等级事件按照系统分类线计组 ·       規则     >     * 公司各称     : 语输入公司名称       报表     *     公司Looo     : 正       报表表     *     公司Looo     : 元       服表力表     *     : 请输入中英文、数字、或英文、: 0符号 量大的字符     *       合 警     >     : 请输入中英文、数字、或英文、: 0符号 量大的字符     *       原格     >     : 直接300个字符     *       系統     >     主申任务     : □	状态 分析 〒	> > > >	图表名称	:	推示框 <u>且示全部</u> 注示框 <u>且示全部</u> 注示框 <u>且示全部</u> 常级事件按算件类型排行  网络绘画事件按照导作类型排行OPI0  《例算件指势 安全设备高等级事件按照系统分类统计	
水 パ     * ▲ 16 8 **     * ▲ 16 8 **       报表     *     *       現表的     *     *       現表的     *     *       日 谷     *       新規、A 16 16 **     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷     *       日 谷   <	资产	>	↓八司々わ		网络设备高等级事件按照系统分类统计图 ▼	
批表的块       * 批表名称       : 请输入中英文、数字、或英文: 0 符号 最大50字符       添加公司logo         合 警       >       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #       #	报表	~	公司LOGO		An BUL AN FEMALES.	~ ¢
古 智 / 現表描述 : 最多300个字符 系统 >	报表列表		* 报表名称	:	请输入中英文、数字、或英文,:0符号 最大50字符	添加公司logo
系 统 >	古 晉 网络	>	报表描述	:	最多300个字符	
	系 统	>	定时任务	:	] <b>#</b> 8	

#### 9.2 删除报表

点击报表列表标题行左侧的复选框,可选中该页所有报表信息,点击每条报表信息左侧 的复选框则可选中该条报表信息→点击报表列表右上角'删除'按钮,系统提示:确定删除 所选项吗?点击'确定',完成批量删除报表的操作。点击每条报表信息'操作'列'删除' 图标,系统提示:确定删除此项吗?点击'确定',完成删除报表的操作。系统内置的报表不 支持删除。

		K				
		报表	自定义报表 搜索关键词	Q	开始时间	- 结束时间 + 3
₩ 状态		🗀 基础审计	□ 报表名称	报表本型	已生成报表	操作
山 分析	>	□ 系统审计		Ministry (V) 472 ally	*****	A. 4 A.
		🗂 WEB审计	, test	目走入报表	木生成报素	
启审计	>	🗂 Windows审计			1	共计 1 条
<b>然</b> 关系	>	□ 流量审计	1			
and the sec		□ 等保合規				
8 用户	>	I SOX合規				
1 资本	,	🗖 IS027001…				
<u> </u>		➡ PCI合规				
◇ 规则	>	□ 其他				
â <u>+</u>		自定义报表				
目报表	Ň					
报表列表						
☆ 告 警	>					
₩ 网络	>					

## 9.3 预览/下载/生成报表

点击每条报表信息'操作'列'生成'图标和'报表生成时间'列的'预览/下载'图标,

※ 总机电话-- 0755-83658009
 ※ 技术支持-- 0755-83658229
 ※ 24 小时技术值班热线-----135-1069-3536
 ● http://www.anysec.com
 ● 深圳市龙华区观澜街道观光路 1301-80 号电子科技大学(深圳)高等研究院 3 号楼 1401



#### 可进行报表的预览/下载/生成操作。

2021-02-20 13:30:2	1	₩ (+) 报表列表						
<b>同</b>		报表	今日事件分析 搜索关键词	Q		开始时间		结束时间
		□ 基础审计	报表名称	报表类型	已生	成报表		脚际 生成
山 分析	>	今日事件分析	基础审计事件发生数(资产)	内置报表	20	21-02-20 14:34:02 ∨	1	BRED/
启审计	>	登录认业分析	基础审计事件发生数(事件子类型)	内置报表	未生	成报表	预监	1 00
		□ 系统审计	基础审计事件发生数(趋势)	内置报表	未生	成报表		下载 🖻 🖉
23。 天 糸	>	■ WEB审计	基础审计事件发生数(资产类型)	内置报表	未生	成报表		00
3.用户	>	🛅 Windows mit	基础审计事件发生数(事件类型)	内置报表	未生	或报表		0
墨 资 产	>	□ 流量审计	基础审计事件发生数(事件级别)	内置报表	未生	成报表		D 0
		□ 等保合规						
▶ 规则	>	□ SOX合规			1			共计 6 务
报表	~	□ IS027001…						
报表列表		□ 其他						
3 告 鑿	>	自定义报表						
9 网络	>							
系统	>							

(注: 先点击生成报表才会出现预览下载删除功能)



十. 告警

菜单项'告警'→'告警信息'子项。进入告警信息列表展示页面。

# 10.1 钻取告警关联事件

点击每条告警信息'操作'列的'查看'即可查看该条告警信息的详细情况。

1-02-20 15:51:46	₩ + + + + + + + + + + + + + + + + + + +							數据导出:	请选择导出
状态	查询条件	and a state of the	and Canon as have						
分析 >	<b></b>	· · · · · · · · · · · · · · · · · · ·	授新大雄子						<b>、</b> 更多余
审计 >	台書列表							点	长钻取
1. m	- 告警名称	告誓类型	告警子类	时间范围	生成时间	告警级别	处理情况	告誓内容	操作
天系	□ 系统磁盘信息 □	. 就据清理			2021-02-20 14:5	重要	木処埋	目前報查谷重超过規定报。	***
用户 >					2021-02-20 14:5***	12.55 10.05	未处理	当前徽盘谷重随过规定报:	* @
资产 >	- 五体磁舟信言	5 5132/前注 1 数据清理			2021-02-20 14:4-	***	未处理	当前截至容量超过从定该	• • •
短 回 >	系统磁盘信息	. <u>如服清理</u> . 對振清理			2021-02-20 14:4	重要	未处理	当前磁盘音量超过从定址	· •
110 114	□ 系统磁盘信息	8. 数据清理			2021-02-20 14:4	重要	未处理	当前磁盘容量超过规定报·	· 🎤 🔊
报表 >	□ 系统磁盘信息	8. 数据清理			2021-02-20 14:4	重要	未处理	当前磁盘容量超过规定报·	· *8
告警~	_ 系統磁盘信』	8. 数据清理			2021-02-20 14:4	重要	未处理	当前磁盘容量超过规定报·	· *8
告警信息	□ 系统磁盘信息	. 数据清理			2021-02-20 14:4	重要	未处理	当前磁盘容量超过规定报·	. *8
告警通知	□ 系统磁盘信息	8. 数据清理			2021-02-20 14:4	重要	未处理	当前磁盘容量超过规定报·	*8
网络 >	□ 系统磁盘信息	B. 数据清理			2021-02-20 14:4	重要	未处理	当前磁盘容量超过规定报·	*8
系统 >					1				井井 11
	30 20 10 0	使用率  70 64.6%  100	0 80 90		- 27 SAL 12	360M —			
t使用率 (单位:百;	分比)			双張盘总量: 9	已用:146,占比	21496			

※ 总机电话-- 0755-83658009∰ http://www.anysec.com



# 10.2 告警通知

菜单项'告警'→'告警通知'子项。进入告警通知列表展示页面。

2021-02-20 15:52:	29	▶ 🕀 🕀 告營通知信息				
同步本		告書通知信息 搜索关键词	Q			ន
		□ 通知名称	邮箱	状态	通知时间	操作
山 分析	>					
自审计	>					
<b>X</b> 关系	>					
8 用户	>					
■ 资产	>					
◇ 规则	>					
报表	>					
☆ 中間	~					
告警信息						
告警通知						
● 网络	>					
(3) 系统	>					



# 十一. 网络

### 11.1 组件状态

菜单项'网络'→'组件状态'子项。进入组件状态展示页面。可查看系统各项功能服 务是否正常。

2021-02-22 10:20:18		₩ ④ 组件状态							
启审计	>	CPU服务		系统服务		数据库服务		升级程序	
		组件状态	正常	组件状态	正常	组件状态	正常	组件状态	正常
20 关系	>	扫描客户端		分布式搜索服务		关联规则服务		日志解析服务[0]	
8 用户	>	组件状态	正常	组件状态	正常	组件状态	正常	组件状态	正常
<b>三</b> 资产	>	wni采集服务		磁盘空间					
A. +0 04		组件状态	正常	组件状态	正常				
V 7/2 /U	<i>,</i>								
會 报表	>								
♥ 告警	>								
@ 网络	~								
如件状态	-								
网络设置									
路由设置									
通信设置									
③ 系 统	>								

### 11.2 网络设置

菜单项'网络'→'网络设置'子项。进入网卡列表展示页面。点击操作列'编辑'图标,可编辑对应网卡信息。



2021-	-02-20 13:41:35		₩ ④ 网络设置						
			同卡列表						
×	关系	>	网卡名称	IP地址	子网掩码	状态	主 <b>DWS</b>	备DNS	操作
8	用户	>	eth0	192.168.1.147	255, 255, 192, 0	Ø			0
101	资产	>						/	
$\diamond$	规则	>							
	报表	>							
P	告警	>							
۲	网络	~							
	组件状态								
	网络设置								
	路由设置								
	通信设置								
0	系统	>							

2021-	02-20 13:41:57		(← ⊕ 网络设置						
			编辑eth0网卡						
×	关系	>	* IP地址	: 192.168.1.147					
8	用 户	>	* 子网捕码	: 255. 255. 192. 0					
	资 产	>		10					
$\diamond$	规则	>	±DNS	: 19]: 180, 70, 70, 70					
Â			番DNS	: 例: 180.70.70.70					
1	抱 衣	<i>'</i>				揚	交 取消		
1	告 警	>	网卡列表						
۲	网络	~	网卡名称	IP地址	子网掩码	状态	主dws	备DHS	操作
	组件状态	_	eth0	192.168.1.147	255. 255. 192. 0	ø			Ø
	网络设置								
	路田 议宣 通信设置								
@	系 统	>							

# 11.3 路由设置

菜单项'网络'**→**'路由设置'子项。进入路由设置展示页面。点击右上角'添加'图标,可添加路由。



2021-02-22 10:25:24	K-€	₽ 略由设置						
@ 审计	> 🚨	<b>念略由设置</b>						-
<b>数</b> 关系	, E	目标网络	子网掩码	下一跳	网卡名称	优先级	状态	操作
	19	92.168.0.0	255. 255. 192. 0	0. 0. 0. 0	eth0	0	U	
各用户	>							
■ 资产	>							
◇ 规则	>							
报表	,							
● 告警	,							
组件中大								
网络设置								
路由设置								
通信设置								
③ 系统	>							
添加静态路由								
* 目标网络	:	请输入目标网络						
* 子网撤码		请输入子网擁码						
*下一跳	;	请输入下一跳						
* 网卡名称	:	eth0				~		
* 优先级	:	请输入优先级						
					提交取消			

# 11.4 通信设置

菜单项'网络'→'通信设置'子项。进入 Syslog 设置列表, SNMP 设置和 session 超时时间设置页面。其中 Syslog 设置可添加删除,所有设置项均可编辑。

2021-02-20 15:02:16		← ⊕ 通信设置				
図 状态		Syslog设置				+
		服务器IP	端口		发送类型	操作
山 分析	>					
自审计	>	SHEP设置				
<b>X</b> 关系	>	团体名称				操作
冬用户	>	las. snapd				Ø
<b>論</b> 资产	,	SHIP Trap 设置				
◇ 规则	>	团体名称				操作
报表	>	snapLog@lqaz				Ø
➡ 告 聲	>					
		session超时时间设置				
● 网络	~	session超时时间				操作
组件状态		30 分钟				Ø
网络设置						
路由设置		日志转发配置列表				+
		转发ip	转发端口	转发协议	备注	操作
\$ <u>\$</u> 3 系 筑	,					

※ 总机电话-- 0755-83658009∰ http://www.anysec.com



# 11.4.1 添加 syslog

点击 Syslog 设置模块的右上角的'添加'图标,展示 Syslog 设置界面,正确填写必要信息,点击'提交'完成添加 syslog 的操作。

IP		端口	发送类型	
log				
∗服务器IP	:	例: 192.168.168.168		
* 服务器端口	:	例: 8080		
* 发送类型	:	请选择(可多选)	•	
			提交取消	

# 11.4.2 编辑 SNMP

点击 'SNMP 设置'模块表格的操作列'编辑'图标,显示 SNMP 设置界面,编辑完成点击 '提交'完成编辑 SNMP 操作。

SNMP设置			
团体名称			操作
las.snmpd			- 0
编辑SNITP团体名			
*团体名称	: las.snmpd		
		趙章	

# 11.4.3 编辑 Session 时间

点击 'session 超时时间设置'模块表格的操作列'编辑'图标,显示 session 超时时间设置界面,编辑完成点击'提交'完成编辑 session 时间操作。

	操作
\$	
报交 — 取消	
	<i>分</i> 提文 <b>联</b> 演



# 十二.系统

#### 12.1 邮箱设置

菜单项'系统'→'邮箱设置'子项。进入告警邮箱设置页面,填写必要的提交信息, 如果选择'启用密码认证',则'SMTP密码'项也作为必填项。

邮箱设置	
* SMTP地址	: 例: smtp.163.com
★ SMTP端口号	: 例: 25/405
* 发件人账户	: 例: las_alert@163.com
* 密码/授权码	: 请输入密码/授权码
启用SSL认证	
	测试 提交

#### 12.2 采集器管理

菜单项'系统'→'采集器管理'子项。进入采集器列表界面。

采集器列表         搜索关键词           □         采集器名称	Q					
□ 采集器名称						-
	采集器IP	采集器端口	采集器状态	采集器运行状态	日志数量	操作
✓ 本机采集器	127. 0. 0. 1		正常	2	10474	
			1			共计 1



### 12.2.1 添加采集器

点击采集器列表右上角'添加'图标,进入添加采集器界面,按要求填写提交项信息→点 击'可用性测试',测试通过显示'提交'按钮→完成添加采集器的操作。

127. 0. 0. 1		正常 1	Ø	10474	## 1
		1			井井 1
					71.
: 请输入中英文、数字、或英文_	:〇符号 最大50字符				
: 例: 192.168.168.168					
: 例: 59000					
: 最多输入300个字符					
	<ul> <li>请输入中英文、数字、或英文_</li> <li>例: 192, 168, 168, 168</li> <li>例: 59000</li> <li>最多输入300个字符</li> </ul>	: 请输入中英文、数字、或英文:0符号 最大50字符 : 例:192.108.108.108 : 例:59000 : 最多输入300个字符	<ul> <li>: 请输入中英文、数字、或英文,:0符号 最大50字符</li> <li>: 例:192.168.168.168</li> <li>: 例:59000</li> <li>: 最多输入300个字符</li> </ul>	: 请输入中英文、数字、或英文:0符号 最大50字符 : 例:192.168.168 : 例:59000 : 最多输入SOO个字符 // 可用性测试 取消	: 请输入中英文、数字、或英文:0符号 最大50字符 : 例:192.168.168.168 : 例:59000 : 最多输入S00个字符

### 12.3 插件中心

菜单项'系统'→'插件中心'子项。进入插件列表界面。点击每条插件信息'操作'列'下载'图标,可下载对应的版本的插件。

2021-02-20 15:18:38	₩ ① 播件中心			
	插件列表			
● 网络 >	文件名称	版本号	描述	操作
③系统 ~	windows agent	V 2.1 build 2019-09-10	采集windows系统日志/网络数据包/应用文件日志	ı.
邮箱设置	Windows agent server 2003 支持包	V 1.0 build 2019-07-10	server 2003 PowerShell 支持包	Û
数据索引信息	windows agent xp 支持包	¥ 1.0 build 2019-07-10	xp PowerShell支持包	Ē
采集器管理		1		共计 3 条
插件中心				
知识库				
日志摘要			占丰下ま	带生
数据库守入 口士			二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	
日主临测				
数据备份				
许可信息				
ping工具				

### 12.4 知识库

菜单项'系统'→'知识库'子项。进入知识库模块页面。

※ 总机电话-- 0755-83658009
 ※ 技术支持-- 0755-83658229
 ※ 24 小时技术值班热线-----135-1069-3536
 ● http://www.anysec.com
 ● 深圳市龙华区观澜街道观光路 1301-80 号电子科技大学(深圳)高等研究院 3 号楼 1401



2021-02-20 15:19:3	1	K⊕	知识库			
		知识唐	列表 搜索关键词	Q		+ ×
● 网络	>	0	经验名称	经验创建时间	经验额述	操作
② 系 统	~		P5负载均衡日志配置远程Syslog采集	2017-04-18 19:24:45	本文将指引你:如何对F5负载均衡日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心…	0
邮箱设置			Cisco交换机路由器日志配置远程Syslog采集	2017-04-18 16:21:20	如何对Cisco交换机/路由器曰志进行采集,并通过Syslog协议,自动实时的发送到远程的集中曰志分析中心,便于…	0
数据索引信			任意文本日志配置远程Syslog采集	2017-01-11 17:02:59	如何对任意文本内的日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式…	0
采集器管理			Tomcat日志配置远程Syslog采集	2017-01-11 17:02:09	如何对Toncat日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式的日志…	0
插件中心			Nginx日志配置远程Syslog采集	2017-01-11 17:01:10	如何对Nginx日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式的日志…	0
知识库			Linux系统日志配置远程Syslog采集	2017-01-11 17:00:18	如何对Linux系统日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式的…	0
口志摘要 約据底导入			Apache日志配置远程Syslog采集	2017-01-11 16:49:21	如何对Apache日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式的日志…	0
日志导入			AIX系统日志配置远程Syslog采集	2017-01-11 16:45:53	本文将指引你: 如何对IBM AIX系统曰志进行采集,并通过Syslog协议,自动实时的发送到远程的集中曰志分析中…	0
日志监测					1	共计 8 条
数据备份						
许可信息						
ping工具						
关机重启						

# 12.4.1 添加经验

点击知识库列表右上角'添加'图标,进入添加经验界面,按要求填写提交项信息→点击'提交'完成添加经验的操作。

021-02-20 15:20:41		ĸ⊕	知识库			
		知识库	列表 搜索关键词	Q		+ ×
)网络	>		经验名称	经验创建时间	经验概述	操作
♀ 系统	~		P5负载均衡日志配置远程Syslog采集	2017-04-18 19:24:45	本文将指引你:如何对P5员载均衡日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心…	0
邮箱设置			Cisco交换机路由器日志配置远程Syslog采集	2017-04-18 16:21:20	如何对Cisco交换机/路由器日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于…	0
数据索引信息			任意文本日志配置远程Syslog采集	2017-01-11 17:02:59	如何对任意文本内的日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式…	0
采集器管理			Tomcat日志配置远程Syslog采集	2017-01-11 17:02:09	如何对Toncat日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式的日志…	0
插件中心			Nginx日志配置远程Syslog采集	2017-01-11 17:01:10	如何对Mginx日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式的日志…	0
知识库			Linux系统日志配置远程Syslog采集	2017-01-11 17:00:18	如何对Linux系统日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式的…	0
日志 摘要 粉 提 底 号 入			Apache日志配置远程Syslog采集	2017-01-11 16:49:21	如何对Apache日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式的日志…	0
日志导入			AIX系统日志配置远程Syslog采集	2017-01-11 16:45:53	本文将指引你:如何对IBM AIX系统日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中…	0
日志监测					1	共计 8 条
数据备份						
1						





# 12.4.2 预览经验

#### 点击每条知识库信息'操作'列'查看经验'图标,可查看该条知识库的详细信息。

知识库	列表 搜索关键词	Q		+ ×
	经验名称	经验创建时间	经验概述	操作
	F5负载均衡日志配置远程Syslog采集	2017-04-18 19:24:45	本文将指引你:如何对F5贷载均衡曰志进行采集,并通过Syslog协议,自动实时的发送到远程的集中曰志分析中心…	0
	Cisco交换机路由器曰志配置远程Syslog采集	2017-04-18 16:21:20	如何对Cisco交换机/路由器曰志进行采集,并通过Syslog协议,自动实时的发送到远程的集中曰志分析中心,便于…	0
	任意文本日志配置远程Syslog采集	2017-01-11 17:02:59	如何对任意文本内的日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式…	0
	Tomcat日志配置远程Syslog采集	2017-01-11 17:02:09	如何对Toncat日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式的日志…	0
	Nginx日志配置远程Syslog采集	2017-01-11 17:01:10	如何对Nginx日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式的日志…	0
	Linux系统日志配置远程Syslog采集	2017-01-11 17:00:18	如何对Linux系统日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式的…	0
	Apache日志配置远程Syslog采集	2017-01-11 16:49:21	如何对Apache日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中心,便于集中式的日志…	0
	AIX系统日志配置远程Syslog采集	2017-01-11 16:45:53	本文将指引你:如何对IBM AIX系统日志进行采集,并通过Syslog协议,自动实时的发送到远程的集中日志分析中…	0
			1 点击预览	共计 8 条

## 12.5 日志摘要

#### 菜单项'系统'→'日志摘要'子项。进入日志摘要模块页面。

2021-02-20 15:25:22	K⊕	日志摘要				E
	日志	简要列表 开始时间 - 结束	时间			
● 网络	<b>`</b>	任务名称	创建时间	状态	进度	操作
⑦ 系统	~ 0	日志摘要任务 2021-02-19 14:37:20	2021-02-19 14:38:46	完成	進度(	ē 💼
邮箱设置		日志摘要任务 2021-02-19 14:30:09	2021-02-19 14:37:34	完成	进度(	愈曲
数据索引信息				1		共计 2
采集器管理						
插件中心						
知识库						
日志摘要						
数据库导入						
日志导入						
日志监测						
数据备份						
数据备份 许可信息						
数据备份 许可信息 ping工具						

### 12.5.1 添加日志摘要

点击日志摘要列表右上角'日志摘要'按钮,进入添加日志摘要界面,选择必要提交项→ 点击'启动'完成添加日志摘要的操作。

2021-02-20 15:28:50 健 网络 >	) 日志擁要 (容特 ) (注意々か) (10年1月)	BEAD (1929) BEAM	
<ul> <li>※ 系 統 ~</li> <li>邮箱设置</li> <li>数据索引信息</li> <li>采集器管理</li> <li>通件中心</li> <li>知识库</li> </ul>	श्रान्थमः : गण्डमा vindows2012	世外生命 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	
日志摘要 数据库导入 日志导入	时间范围 : 近1分钟	2	~

### 12.5.2 日志摘要删除

点击日志摘要列表标题行左侧的复选框,可选中该页所有日志摘要,点击每条日志摘要 左侧的复选框则可选中该条日志摘要→点击日志摘要列表右上角'删除'按钮,系统提示: 确定删除所选项吗?点击'确定',完成批量删除日志摘要的操作。点击每条日志摘要信息'操 作'列'删除'图标,系统提示:确定删除此项吗?点击'确定',完成删除日志摘要的操作。

日志排	著要列表 开始时间 - 结束时间	Q			→×
	任务名称	创建时间	状态	进度	操作
	日志摘要任务 2021-02-19 14:37:20	2021-02-19 14:38:46	完成	进度 100%	D. 🗇
	日志摘要任务 2021-02-19 14:36:09	2021-02-19 14:37:34	完成	进度(	<u>۵</u>
			1		共计 2 条

# 12.5.3 日志摘要下载

点击每条日志摘要信息'操作'列'下载'图标,系统提示:确定下载该条任务结果吗? 点击'确定',完成下载日志摘要的操作。

日志拔	要列表 开始时间 - 结束时间	<mark>م</mark>			×
	任务名称	创建时间	状态	进度	操作
	日志摘要任务 2021-02-19 14:37:20	2021-02-19 14:38:46	完成	进度 100%	D 🗇
	日志摘要任务 2021-02-19 14:36:09	2021-02-19 14:37:34	完成	进度 (	意意
			1		共计 2 条

## 12.6 数据库导入

菜单项'系统'→'数据备份'子项。进入数据库导入模块。



2021-02-22 10:38:54		
● 网络 >	32篇4947 透耀文件 未选择任何文件	
③系统 ~		
邮箱设置		
数据索引信息		
采集器管理		
插件中心		
知识库		
日志摘要		
数据库导入		
日志导入		
日志监测		
数据备份		
许可信息		
ping工具		
关机重启		

# 12.7 日志导入

菜单项'系统'→'日志导入'子项。进入日志导入模块。选择'关联设备类别',上传 完整日志.log 文件,点击'提交'按钮,完成日志导入操作。

2021-02-20 15:45:35	
	日志9入
④ 网络 >	关联资产类别 : 请选择 🗸
③系统 ~	关联资产类型 : 请选择 🗸
邮箱设置 数据索引信息	选择文件 : 选择文件 未选择任何文件
采集器管理	構立
插件中心	_
知识库	
日志摘要	
数据库导入	
日志导入	
日志监测	
数据备份	
许可信息	
ping工具	
关机重启	

#### 12.8 日志监测

菜单项'系统'→'日志监测'子项。进入日志监测模块。可以监测系统是否可以采集 到客户端日志。

	④ 日本培諭			
2021-02-22 10:39:44	★ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	求验证 (如:火薬湖览器)。若日志监测无法正常使用,请点击满加喻证。		
● 网络 >	UDP V 请输入源IP地址	请输入目标IF地址	请输入目标端口(514)	
③ 系 統 ~  師箱设置 数据索引信息 采集器智道 猫保中中心 知识成準 日志規葉 入 日志导入				
日志导入日志监测	1			
许可信息				
ping工具 半机蛋白				

# 12.9 数据备份

	10 4 10 4 10 10 10 10 10 10 10 10 10 10 10 10 10				宙伤/清理: -请选择- V	の単の「日初海理」「日
- 14 N	與馬苗折列表 搜索大键词	Q				
网 3合 7	记录名称	记录时间	记录大类	记录状态	索引名称	操作
系统 >	日志(其它)备份	2021-02-20 15:34:35	日志(其它)	未完成	las-e-2021-02-19, las-e-2	021-02-0
邮箱设置				1		共计 1 ई
数据索引信息						
采集器管理						
插件中心						
知识库						
日志摘要						
数据库导入						
日志导入						
日志监测						
数据备份						
许可信息						
ping工具						
关机重启						

菜单项'系统'→'数据备份'子项。进入数据备份模块。

# 12.9.1 手动备份

按需选择页面右上角'备份/清理'项,系统提示:确定备份此项吗?点击'确定'完成 手动备份操作。
		5					客	Anysec techn
2021	1-02-20 15:37:10		₩ ● 数据备份				备份/清理:请选择- V	目动番份 自动清理 自动转
۲	网 络	>	数据备份列表 搜索关键词 记录名称	记录时间	记录大类	记录状态	数据(F(生前) 日志(其它) 達建数据(其它) 家一百研	操作
(ĝ)	系统	~	日志(其它)备份	2021-02-20 15:34:35	日志(其它)	未完成	as-e-2021-02-19, las-e-	-2021-02-0
	邮箱设置					1		共计 1 条
	数据案引信息 采集器管理							
	插件中心							
	知识库							
	日志摘要							
	数据库导入							
	日志导入							
	日志监测	_						
	数据备份							

#### 12.9.2 自动备份

点击右上角'自动备份'按钮,显示自动备份模块,按照需要勾选或填写提交项信息, 点击'提交'按钮完成自动备份操作。

2021-02-20 15:38:16	← ⊕ 数据备份				备份/清理: -请选择- 🗸	自动备份 自动清理 自动转存
	数据备价列表 搜索关键词	٩			/	
④ 网络 >	记录名称	记录时间	记录大类	记录状态	索引名称	操作
③系统 ~	日志(其它)备份	2021-02-20 15:34:35	日志(其它)	未完成	las-e-2021-02-19, las-	e-2021-02-0
邮箱设置			1			共计 1 条
数据索引信息						
采集器管理						
插件中心						
<b>山</b> 以库 日主擁更						
H 10110 SK						
自动备份功能						
是否开启	: 🗹					
,夕心光到		<b>- -</b> +				
* 留历尖型	: 🗹 數据库					
* 初始备份开	始时间 :					
* 执行时刻	:					
	3+14.3.+5.91					
* 备份间隔	: 请输入整数			天	~	
				提交 1 1	网络	
				1/2.2		

### 12.9.3 自动清理

点击右上角'自动清理'按钮,显示自动清理模块,按照需要勾选或填写提交项信息, 点击'提交'按钮完成自动清理操作。



2021-02-20 15:44:00		₩ 🕀 🕀 数据备份					备份/清理	1: -请选择- ✓ 自动备份 自該	动清理 自动转存
		数据备份列表 搜索关键	a)	٩					
● 网络	>	记录名称	记录时间		记录大类	记录状态		索引名称	操作
③ 系统	~	日志(其它)备份	2021-02-20	15:34:35	日志(其它)	完成		las-e-2021-02-19, las-e-2021-02-0…	1001
邮箱设置					1				共计 1 条
数据索引信息									
采集器管理									
插件中心									
知识库									
日志摘要									
<u></u> 知道库寻八 日志島λ									
日志监测									
数据备份									
		(手) 数据备份							
2021-02-20 10:44:09		自动清理功能							
● 网络	>								
Sta # 44		是否升启	: 🗹						
105 MK 90		存储路径	: /usr/local/las/						
即相议宣			文件系统:/dev/sd	.2 目录总量:	926	已使用量: 13G	占用率: 14%		
采集器管理		拉会注册词法	07						
插件中心		* EIM /H/± NUM	: 50					? 	
知识库		* 清理至	: 90					8	
日志摘要		*磁盘告警阈值	: 95					%	
数据库导入		* 保在周期	. 180			Ŧ	~		
日志导入		W IT AND	. 100				-		
日志监测						提交 戰	有		
	-	数据备份列表 搜索关键	词	Q					
ping工具		记录名称	记录时间		记录大类	记录状态		索引名称	操作
关机重启		日志(其它)备份	2021-02-2	) 15:34:35	日志(其它)	完成		las-e-2021-02-19, las-e-2021-02-0…	配心前
					1				共计 1 余

## 12.9.4 自动转存

点击右上角"自动转存"按钮,显示自动转存功能,按照需要勾选或填写提交项信息, 点击'提交'按钮完成自动转存操作。

		数据备价列表 搜索关键词	Q				
● 网络	>	记录名称	记录时间	记录大类	记录状态	索引名称	操作
③ 系统	~	日志(其它)备份	2021-02-20 15:34:35	日志(其它)	完成	las-e-2021-02-19, las-e-2021-02-0	r c f
邮箱设置				1			共计 1 5
数据索引信息							
采集器管理							
插件中心							
知识库							
日志摘要							
数据库导入							
日志导入							
日志监测							
日志监测 数据备份							
日志监测 数据备份 许可信息							
日志监测 数据备份 许可信息 ping工具							

ttp://www.anysec.com

 · 技术支持-- 0755-83658229
 · 24 小时技术值班热线-----135-1069-3536
 · 27 小市龙华区观澜街道观光路 1301-80 号电子科技大学(深圳)高等研究院 3 号楼 1401

功能		
是否开启	:	
* 服务器地址(FTP)	:	例: 192.168.1.1
* 端口	:	请输入端口号
* 用户名	:	请输入中英文、数字、或0@符号 2~20位字符
* 密码	:	请输入密码
*转存路径	:	请输入路径,不支持中文路径

#### 12.10 许可信息

菜单项'系统'→'许可信息'子项。进入系统许可信息模块,可查看系统版本和授权 信息,也可在'注册码'信息表中上传注册文件,点击'授权'完成系统的授权操作。

2021-02-20 15:47:34	₩ (平) 许可信息					
	关于产品					
	版本类型	授权天数	剩余天数	资源数	剩余资源	授权时间
③ 系统 ~	测试版	90	44	50	47	2021-01-05 10:23:51
邮箱设置						
数据索引信息	系统升级					
采集器管理	当前版本			上传升级文件	<b>†</b>	
插件中心	1.0.6.289			选择文件	未选择任何文件	升级
知识库						
日志摘要	修正设备系统时间					
数据库导人	服务器时间	: 2021-02-20 15:47:38				
日志监测						
数据备份	浏览器的时间	: 2021-02-20 15:49:07				
许可信息					修正时间	
ping工具	18-10/5-0					
关机重启	12/02 (6.25					
	* 本机软件序列号	: AD56857A114C877F35D471FADDBF89C2				
	* 授权	: 选择文件 未选择任何文件				
				1= 40	Butan	
				10.02	HILL RANK	

#### 12.10.1 系统升级

菜单项'系统'**→**'许可信息'子项。进入系统升级模块,可查看系统版本和升级信息, 也可'系统升级'表中上传升级文件,点击'升级'完成系统的升级操作。



2021-02-20 15:49:00	₩ (平) 许可信息					
	关于产品					
● 网络 >	版本类型	授权天数	剩余天數	资源数	剩余资源	授权时间
◎ 系统 ∨	测试版	90	44	50	47	2021-01-05 10:23:51
邮箱设置						
数据索引信息	系统升级					
采集器管理	当前版本			上传升级文	t件	
插件中心	1.0.6.289			选择文件	未选择任何文件	升级
知识库						
日志摘要	等止反由系统时间					
数据库导入						
日志导入	脈方詰时间	: 2021-02-20 15:49:00				
日志监测	浏览器的时间	: 2021-02-20 15:50:29				
数据备份						
许可信息					10正町1日	
ping上具	授权信息					
大机里后	* 木机較性度利导	. AD580576114007782504718400880	ac2			
	******************	. RESUSSINITED IN SUPPLY ADDRESS	1962			
	* 授权	: 选择文件 未选择任何文件				
				1巻本0	导生经权	

## 12.11Ping 工具

菜单项'系统'→ 'ping 工具'子项。进入系统 ping 工具模块,可查看设备网络之间连 通性。

2021-02-22 10:17:07	
	ping工具 提示: 个别别员器变美添加ping工具的请求给证(如:火集别员器)。若ping工具无法正常使用,请点请参加证证。
● 网络 >	*ping地址 : 请输入ping地址 [FING
◎系统 ~	
邮箱设置	
数据索引信息	書と作文でになり、なられ
采集器管理	
插件中心	
知识库	
日志摘要	
数据库导入	
日志导入	
日志监测	
数据备份	
许可信息	
ping工具	
关机重启	



# 12.12 关机重启

	₩ + 可信息							
	版本类型	授权天数	剩余天數	资源数	剩余资源	授权时间		
	测试版	90	44		47			
邮箱设置								
	当前版本			上传升级文件				
				选择文件	任何文件			
				$\sim$				
	in the matrix							
	服用器时间	: 2021-02-20 10149141 关闭系	슠	番白系统				
	浏览器的时间	; 2021-02-20 15:51:10	-/6	-11/5-A				
	*本机软件序列号	: AD56857A114C877F35D471FADDBF89C2						
	• 授权	: 选择文件 未选择任何文件						

※ 总机电话-- 0755-83658009 http://www.anysec.com